

## عالم تحليل الشبكات أسس وقواعد

VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
53	283.404390	Vmware_a1:92:d0	Broadcast	ARP	who has 10.0.0.1?
54	287.404329	Vmware_a1:92:d0	Broadcast	ARP	who has 10.0.0.1?
55	288.249376	10.0.0.30	10.0.0.255	BROWSER	Host Announcement
56	821.126463	10.0.0.55	10.0.0.255	BROWSER	Local Master Annnc
57	823.197211	10.0.0.30	10.0.0.255	NBNS	Name query NB TES
58	823.198927	Vmware_c0:00:08	Broadcast	ARP	who has 10.0.0.30
59	823.199870	Vmware_a1:92:d0	Vmware_c0:00:08	ARP	10.0.0.30 is at C
60	823.200917	10.0.0.55	10.0.0.30	NBNS	Name query respor
61	823.204442	10.0.0.30	10.0.0.55	ICMP	Echo (ping) reques
62	823.204551	10.0.0.55	10.0.0.30	ICMP	Echo (ping) reply
63	823.210722	10.0.0.30	10.0.0.55	TCP	nsstn> netbios-s

Frame 55 (243 bytes on wire, 243 bytes captured)

Ethernet II, Src: Vmware\_a1:92:d0 (00:0c:29:a1:92:d0), Dst: Broadcast (ff:ff:ff:ff:ff:f)

Internet Protocol, Src: 10.0.0.30 (10.0.0.30), Dst: 10.0.0.255 (10.0.0.255)

User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)

NetBIOS Datagram Service

SMB (Server Message Block Prot

Wireshark RTP Player

0000 ff ff ff ff ff ff 00 0c 21

0010 00 e5 00 fe 00 00 80 11 21

0020 00 ff 00 8a 00 8a 00 d1 a1

0030 00 1e 00 8a 00 bb 00 00 21

0040 4f 43 41 43 41 43 41 43 41

0050 41 43 41 43 41 43 41 43 41

0060 43 45 4c 45 48 46 43 45 51

From 192.168.2.21:8004 to 192.168.2.12:8046 Duration:13.68 Drop by Jitter Buff:0(0.0%) Out of Seq: 1(0.1%)

From 192.168.2.12:8046 to 192.168.2.21:8004 Duration:13.70 Drop by Jitter Buff:0(0.0%) Out of Seq: 1(0.1%)

Jitter buffer [ms] 50 Decode Play Stop Close

## نتائج الاستفتاء

ماهو تقييمك للمجلة ول محتواها ؟

رائع

78%

جيد

19%

وسط

3%

سيئ

0%

• كيف تحدد أسباب بطئ الشبكة

• الخطوات معالجة المشكلة

• الواير شارك وكيف تتعامل معه



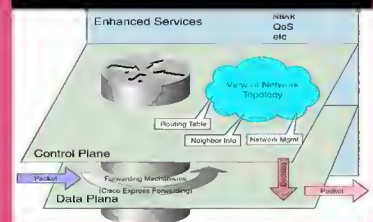
شهادة الـ CCIE

تجربة عملية

نصائح , ملاحظات

تقرأون في هذا العدد

ماهي تقنية الـ CEF وكيف تعمل



Routing Table ونظرة

عن قرب

قصة حياة ملف

سيسكو تعلن الحرب على  
مهربى الأسئلة !تعرف على خاصية الـ Call  
Park في تلفونات سيسكووالعديد من المواضيع  
الجديدة والقيمة

شاهدوا أيضا أقسام

مصطلحات تقنية

عتاد ومعلومات

مشاكل وحلول

6



# أفتتاحية العدد

## اقرأ اقرأ اقرأ

### المحررون الدائمون

- الدكتور محمد التميمي

Yarra\_link@yahoo.com

- المهندس أيمن النعيمي

www.networkset.net

- المهندس أحمد الشحات

warior10@hotmail.com

- المهندس عادل الحميدي

adel\_husni2000@hotmail.com

- المهندس عمر السويدي

om18899@gmail.com

- المهندس أحمد بخيت

www.abakhiet.info

- المهندس محمود عمر

mahmoudomr@gmail.com

- المهندس أحمد الجرجولي

ahm\_ijal@hotmail.com

لماذا عندما أنتهي من مشاهدة الفيديو الخاصة بالكورس وأقوم بالرجوع إلى أسئلة الامتحان أجد نفسي لا أفقه شيء ولا أعلم أي شيء عنها ؟ أحد أكثر الأسئلة شهرة والتي صادفتني في الكثير من المنتديات والمواقع العربية والتي قد تتغير صيغتها أحيانا لكن لمضمون واحد فالجميع يريد أسرع طريقة للحصول على الشهادة لكن بطريقة يقنع نفسه بأنه تعب وتعلم لكي يحصل عليها لذا يلجأ إلى الشروحات والفيديوهات الموجودة والمختصة في هذا المجال والتي توصله لقناعة تامة بأنه أنتهي من دراسة الكورس وأصبح جاهزا للامتحان والتي سوف تكون نقطة التحول بالنسبة لهذا الطالب فعندما يقوم بالأطلاع على الأسئلة سوف يجد أن هناك الكثير من الأشياء المطروحة لا يعلم عنها أي شيء ولم سمع عنها أيضا لذا سوف يكون أمام ثلاث خيارات :

الأول سوف يبدأ في حفظ الأسئلة ورسمها في دماغه مثل قاعدة  $1+1=3$  وهي للأسف النسبة الأكبر منهم الثاني سوف ينصدم من الأسئلة وسوف يعتقد بأن الخلل منه وسوف يبدأ يشك في قدراته وأمكاناته والتي سوف تنتهي بأن يخلق الأسئلة ويقوم بحذف الفيديوهات ويبحث عن شيء آخر ليقوم بدراسته الثالث وهي السؤال الذي تحدثت عنه في أول المقال لماذا أجد الكثير من الأسئلة التي لم أفهم منها أي شيء ولم أسمع عنها إطلاقا ؟

جوابي كان دائما لمثل هذه الأسئلة هو الكتاب ثم الكتاب ثم الكتاب وحقيقة أجد الكثير من الطلاب يبتعدون عن الكتاب لأنه الطريق الأصعب للدراسة وخصوصا أن أغلب الكتب الموجودة باللغة الانكليزية وعلى ما يبدو أن ثقاتنا الانكليزية ضعيفة بعض الشيء لذا نجد طلابنا العرب يتهربون ويبتعدون على الكتاب ونسوا أن الكتاب هو المكان الوحيد الذي يضمن لك المعلومة 100% ويغنيك عن أي شيء آخر أما موضوع الاستفادة من الفيديوهات والشروحات الموجودة فهو مهم لكن اعتبره فقط جسر صغير للعبور إلى المفهوم الأساسي لذلك الكورس فهو إن أعطاك بعض المفاهيم فهي تمثل 60% كحد أقصى لهذا الكورس وبقي عليك الـ 40% والتي سوف تمنحك التمييز والفهم الحقيقي لما تدرسه وفي النهاية المكسب معك لأن التأسيس الصحيح لكورس مثل الـ CCNA سوف يسهل لك دراسة كورسات أعلى منه وسوف يوسع عقلك بشكل أكبر .

خلاصة هذا الكلام وأحب أن أبتدئها بأول كلمة قالها الله عز وجل لنبيينا محمد صلى الله عليه وسلم وهي "اقرأ اقرأ اقرأ" وأسستن بالله وكن ذي إرادة قوية وساهم في رفعة امتنا العربية المسلمة لان بدون القراءة لن نثمر ولا في أي يوم من الأيام وسوف يبقى شعارنا الاستهلاك ونصيحتي لك لو بدأت بقراءة أي كتاب باللغة الانكليزية أن تصبر كثيرا وخصوصا في أول الكتاب لان أغلب الكتب تكون بدايتها كلام نظري ومعقد وسوف تعتاد عليه مع مرور الوقت وخصوصا أن الذي قام بتأليفه هو شخص واحد لذا سوف تعتاد على كلماته وسوف تجد نفسك في تطور ملحوظ وخصوصا إن وصلت لمنتصف الكتاب لانك سوف تجد نفس المصطلحات الذي كنت قد ترجمتها في بداية هذا الكتاب بدأت تتكرر وسوف تتغير نظرتك إلى الكتاب وسوف تبدأ بالشعور باللذة لما تقراء وخصوصا أنك الآن بدأت تفهم ماذا تقرأ والذي سوف ينعكس عليك بشكل إيجابي كبير لان ثقتك في نفسك سوف تزيد وسوف تعلم أن أبواب العلم قد فتحت لك ولن يقف أي شيء في وجهك فتخيل معي أخي العزيز هذا الشعور أي شيء أريد أن أتعلمه أصبح بين يدي وكل ما أحجته هو الكتاب وخصوصا أن الأنترنت قدم هدية كبيرة لنا وهي الكتاب الإلكتروني فكل ماتريده أصبح متوفر عندك وبدون أي عناء وبضغطة زر واحدة سوف تجده أمامك .

أختم كلامي بجاذبة مرت معي منذ أسبوع فإثناء بحثي على الأنترنت وجدت موقع يحوي من الكتب مايسيل لعاب أي شخص محب للقراءة وفي شتى المجالات فوالله ماتمنيت في تلك اللحظة إلا شيء واحد أن أجد الوقت لكي أقرأ كل هذه الكتب فأنتفع بها وأنفع بها من يريد لكن المشكلة كانت أن كل الكتب باللغة الانكليزية وهذا يحتاج مني وقت مضاعف وتمنيت لو كانت كل هذه الكتب موجودة باللغة العربية لكنك أنتهيت منها في شهر واحد لكن لا أخفيكم أن الموقع وضعته في المفضلة عندي وانتظر بعض الوقت لكي أبدأ القراءة .

أيمن النعيمي

موقع المجلة

www.networkset.net

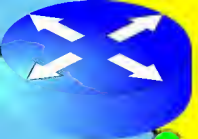
بريد المجلة

magazine@networkset.net

بريدي الخاص

admin@networkset.net

جميع الحقوق محفوظة لكاتبها



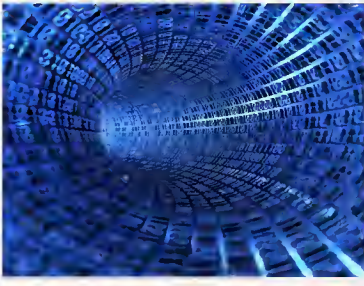
# محتويات أيلول 2110



عالم تحليل الشبكات أسس وقواعد صفحة 6

- |    |  |    |   |
|----|--|----|---|
| 17 | طريقة حفظ وتسرجاع الإعدادات على أجهزة جونيير | 3  | قصة حياة ملف                                    |
| 17 | كيف تقوم بتحويل ويندوز XP إلى روتر           | 4  | Cisco Routing Table نظرة عن قرب                 |
| 18 | كيفية التحويل بين IP4 و IP6                  | 5  | سيسكو تعلن الحرب على مهربي الأسئلة              |
| 18 | الـ PASSIVE INTERFACE وماهي فائدته           | 8  | ماهي تقنية الـ CEF وكيف تعمل ؟                  |
|    | قسم الأمن والحماية                           | 9  | شهادة الـ CCIE تجربة نصائح ملاحظات              |
| 19 | - الطريق إلى السكورتري                       | 10 | أول وأكثر شخص حاصل على شهادة الـ CCIE في العالم |
| 21 | قسم عتاد ومعلومات                            | 11 | من أين وكيف أبدا طريق الشبكات                   |
| 23 | قسم مصطلحات تقنية                            | 12 | نتائج الأستفتاء الشهري                          |
| 24 | قسم مشاكل وحلول                              | 13 | لينكس والشركات الكبرى                           |
|    |  | 14 | تعرف على خاصية الـ CALL PARK                    |
|    |  | 16 | طريقة إعداد الـ STATIC ARP                      |

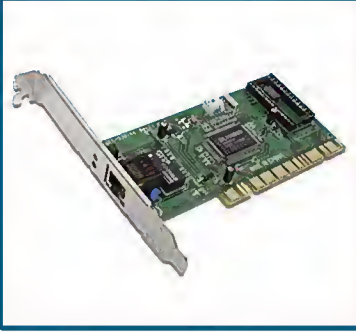




# قصة حياة ملف

بقلم: احمد الجلولي

وبدأت الرحلة حيث وصلت الى المطار ( كرت الشبكة ) وقمت بقراءة التعليمات الخاصه بالسفر والتي تكون على مرحلتين تبدأ في عملية التشفير ( التحول الى نبضات كهربائية ) ومن ثم الركوب بالنافل ( الكيبيل ) حتى الوصول الى الجبهة الاخرى , وبطبيعته الحال تم تشفيري وتحويلي لأدخل من بعد ذلك الى عالم الانتقال بالشبكات وخوض تجارب



تجارب بتلك التكنولوجيا حيث ان جميع درجات السفر موحده ولا يهمهم ما كنت عليه بل ما انت عليه الان والفرق بينك وبين غيرك هو من خلال نوع المركبة التي تستخدمها ( الكوابل ) فهناك العديد والكثير , واخيرا وصلت الى الجبهة المقابلة حيث انها لم تكن الوجهة التي اريد بل هي محطه مركزية رئيسيه عملها هو توزيع المعلومات وارسالها الى الجبهة المحدده لها وطبعاً لا تستطيع اختيار اي جهة بل تختار وجهتك اليا من خلال تلك المحطه واي عصيان للاوامر يؤدي بك الى السجن ( سله المهملات ) .

وهكذا اصبحت هذه الوسيله ( الشبكة ) معروفة وتعد من افضل طرق التنقل واكثرها اماناً وتمتاز بالسرعه والخدمات التي يقدمونها لك اثناء السفر وما يميزها تقديم المشروبات والمأكولات الشهيه ( فحص الفيروس , الترتيب , الحماية ) , وبت انتقل من كيبيل الى آخر فمنها ما هو بطيء وما هو سريع حيث يتم تقسيمها الى فئات عدة تسمى بالتصنيفات العاليه ( Category ) ولها عدة سرعات فمنها يحتاج الى ثانيه لنقل عشره ملفات بحجمي ( 10base-T ) ولا يتجاوز طول الطريق عن مائه متر للوحده , وهكذا حتى تم استخدام كوابل جديده تمتاز بسرعه اكبر حيث انني لا اكد اذكر تلك الاجزاء من الثانيه عند الانتقال بها فهي تحتاج الى نقل مائه ملف بحجمي الى ثانيه واحده فقط ( 100base-T ) والسبب في استخدام هذه السرعه العاليه هو انهم قاموا بإزالة جميع نقاط التفتيش على الطريق وجميع كاميرات السرعه على الطريق ولهذا اصبح السائقون ( Carriers ) يقودون بنا بسرعه جنونيه وبدقه عاليه في القيادة بدون ايه حوادث تذكر .

ومن هذا الى ذاك ومن جهاز لآخر ومن كيبيل الى آخر والعديد العديد من التجارب والى ان سمعت بكوابل تنقل بسرعه عاليه جدا تفوق كل ما سبقها ( Fiber Optic ) حيث انك لا تستطيع ان تصل الى مقعدك فني كل مره استخدم هذه الوسيله ادخل الى المركبه لأجلس على مقعدي ما ان اعبر المدخل فيقولون لي اننا وصلنا وخابت كل امالي بتجربه الجلوس على تلك المقاعد الجليليه الفاخره فكل من كان يجلس عليها هم من اصحاب الاحجام الثقيله والتي ظننت انهم يعملون بوظائف مهمه ولكنهم كانوا يمتلكون احجام ( سعه ) كبيره , وايضا لا توجد ايه مشكله في المسافه التي تقطعها اثناء السفر فهي تصل الى 2 كيلومتر للكيبيل الواحد والسبب هو تزويد النواقل بخزان وقود إضافي لتقطع مسافه اكبر ( Full Duplex ) ليس كالنواقل العاديه ذوات الخزان العادي ( Half Duplex ) .

وفي كل مره يستخدم كيبيل جديد يكون لي الشرف بتجربته وصرت انتقل من منطقه لاخرى ومن بلد لآخر بكل سهوله وحتى اذكر اني استخدمت الطائرات ( Wireless Networks ) للانتقال , وتوالى عمليات النقل الى الان حيث انه لزم نقلي من موقع المجله لاستقر على اجهزتك دقيقه او اقل وانتم الان تستمتعون بقراءتي واتمنى ان اكون ضيفا خفيفا على اجهزتكم والتي اعدكم بانني لن افعل ايه مشاكل فقد اصبحت كبيرا في العمر واتمنى ان لا تنقلوني الى سله المهملات لديكم فأنت تحتاج الى ثانيه لحذي ولكن فكر بكل ذلك الوقت وتلك التكنولوجيا العظيمه التي استخدمتها للوصول إليك . 000011100111

تعرف الى ما يحدث اثناء نقل الملفات من جهاز لآخر عبر الشبكة , وايضا بإمكانك عزيزي القارئ معرفه سرعات كل سلك شبكه وما يميزها عن بعضها فقط من خلال مقابله حصريه مع ملف قمت بها شخصيا وقد جعلته يروي لكم قصته وتجاربه من خلال تفاصيل تنقله واستخدامه للشبكه كوسيله :

00111001101  
عباره عن ملف نصي واسمي الاول هو ( CH ) واسمي الاخير ( اسم العائله ) هو . TXT وابلغ من السعه واحد ميغابايت ( 1 Mb ) ولكن ما يميزني هو انني اخيرا سأروي قصتي لكم عبر هذه المجله الرائعه , وذلك كما اخبرني صديق لي كان دائما متابعا ويقرأ كل عدد منها واسمه ( Adobe Reader ) الامر الذي اثار الفضول بداخلي لكنني بالحقيقه لا استطيع القراءه حيث انه كما تعلمون عني فقط اقرأ ما يكتب بداخلي , وتوجد هنالك العديد من البرامج المعالج للصوص والتي تستطيع قرائتي



والان اتمنى ان لا اكون قد اطلت عليكم في التعريف بنفسني ولكن لا اعرف من اين ابدا فهذه هي التجربه الاولى في حياتي التي استطيع من خلالها التكلّم , فقد تم انشائي في عام 1986 على جهاز حاسب الي حيث انني كنت اعيش على القرص الصلب واذكر انذاك انه عندما كان يأتي امر بنقلي او بقرائتي كنت اعاني من ذلك المعالج العجوز البطيء ولكن مما اذكر انه لم تكن انذاك اي وسيله لنقلنا ( انا وغيري من الملفات الاخرى ) من جهاز الى آخر إلا وسيله النقل العام ( Floppy Disk ) وهذه الثقليات اعترف انها بطيئه والقرص الواحد منها لا توجد لديه القدره على نقل الكثير منا لانه دائما يقول لا توجد اماكن اخرى ( A Disk is Full or WriteProtected ) ولكن اذا اقتضت الحاجه الى ذلك يجب ان ادخل اولاً فيما يسمى ببرنامج ضغط ( WinZip ) وهذا عباره عن شخص لديه خبره طويله في التعامل مع دائره الجمارك ( محرك الـ Floppy ) ودائماً كان يضع ملفات بضغفي حجمي في ملف واحد ( ZIP ) ولا تتجاوز سعته نصف سعتي ( لا ادري كيف كان يهرب الملفات ) وبعد ذلك الامر بمدته سمعت بأن المعالج العجوز قد انتهى امره ( الله يرحمه ) الامر الذي جعلنا جميعاً نستخدم الكثير من وسائل النقل العام ( اقراص الـ A ) لننتقل الى جهاز حاسوب جديد حيث انه من شدة الاستعجال تم تقسيمي الى قسمين كل قسم بقرص وانا الان احذركم عبر قسمي الاول ولا ادري اين قسمي الاخر ( الى الان ابحت عنه ) .

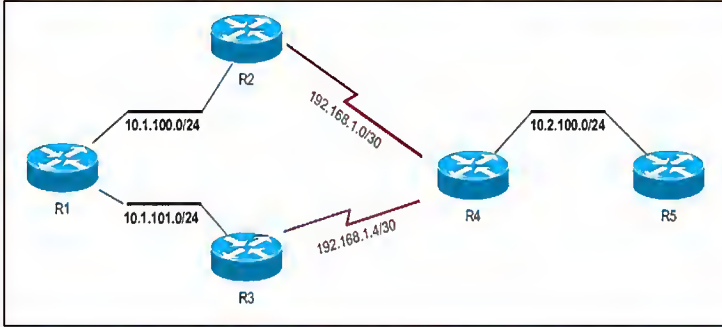
واذن تم نقلنا الى جهاز حاسوب جديد ذو معالج مطور حيث انه في البدء عند وصولنا إليه اخذ يطرح علينا اسئله كثيره وكان دائماً يقول : هذا الامر ليس بيدي ولكن لكي استطيع الاجابه على اسئله المستخدم ولكن ما فاجئتني دائماً هو تلك السرعه التي تنتقل عليها الملفات من جهاز لآخر عبر ما يعرف بالاقراص المدمجه ( CD ) واخبرني ملف اخر بأنه عندما ينتقل عبر هذه الوسيله هنالك درجات ومقاعد محجوزه مسبقاً لكل شخص حسب اهميته طبعاً ولكن يشترك الجميع باله الدغدغه الليزرية ( العدسه ) وركوب لعبه الملاهي ( دوران القرص اثناء قرائته ) ولكن انا اختلف عن الجميع حيث انني لم اجرب تلك الوسيله لكن هنالك وسيله اخرى فاخره قمت بتجربتها ( اخيراً موضوع القصه ) حيث انه في يوم من الايام جاء الامر اخيراً بنقلي من هذا الحاسب الى اخر عبر ما يسمى بالشبكه ( Network ) واذكر بأن جميع الملفات الاخرى قاموا بتنهنّتي لذلك ( وبعضهم حسدني ) وجاء ذلك اليوم الذي سوف انتقل فيه لتبدأ رحله طويله لم اكن اعرف بأنها سوف تكون شاقه .



# Routing Table Cisco

## نظرة عن قرب

بإسم: أحمد مصطفى



وفي المثال الثالث كل الجمل تحتوي علي ال Next Hop Ip Address وبالتالي أيضاً تعتبر Ultimate.

وقبل البدء في تعريف ال Routes في هذا المستوى تجدر بنا الإشارة إلي تعريف ال Parent Route.

Parent Route: وهو ال Route الذي يحتوي على ال subnet mask أكبر من ال default subnet mask للفئة التي ينتمي لها، فمثلاً: نلاحظ أن الجملة الأولى في المثال التالي وهي 172.16.0.0/24، نلاحظ أنها تحتوي على ال subnet mask يساوي 24 وهو بالطبع أكبر من ال default subnet mask والذي يساوي 16.

Ex:4

```
RouterB#show ip route
<text omitted>
172.16.0.0/24 is subnetted, 3 subnets
R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:20, Serial0
C 172.16.2.0 is directly connected, Serial0
```

بعد أن انتهينا من تعريف ال parent route إذن ما هي ال Routes في المستوى الثاني:

المستوي الثاني Level Two:

هذه ال Routes تسمى ال Childs وهي تقع مباشرة تحت ال Parent وهي تعتبر Subnet من ال Classful Network Address والذي يمثل ال Parent.

وهنا عندنا حالتين:

- حالة ال Classful

- حالة ال Classless

1- حالة ال Classful كما في المثال الرابع، حيث يشير ال Parent في الجملة الأولى إلي أنه is subnetted, 3 subnets وعلى ذلك يحتوي ال Parent فقط على ال Subnet Mask ولا يحتوي أي من ال Childs على ال Subnet Mask.

2- حالة ال Classless كما في المثال التالي "المثال الخامس"، حيث يشير ال Parent في الجملة الأولى إلي أنه is subnetted, 2 subnets، 2 masks أي أنه يشير إلي استخدام ال VLSM.

وفي هذه الحالة يحتوي ال Parent على ال default subnet mask وهو في هذا المثال 16/ وبالتالي يحتوي كل ال Child على ال subnet mask الخاص به كما في المثال.

إن القدرة على سرعة ترجمة الجمل الموجودة في ال Routing Table من المهارات الأساسية لدي حاملي شهادات سيسكو وهذه الجمل لها قواعد معينة نسير عليها في عملية ترجمة هذه الجمل.

ولنبدأ ببعض التعريفات الأساسية التي سوف تساعدنا إن شاء الله في فهم هذه الجمل. يمكن تقسيم ال Routes في الجدول إلي مستويين:

المستوى الأول Level one

وهو كل Route يحتوي على ال subnet mask مساو أو أقل من ال default subnet mask لهذه الفئة Class. فمثلاً عند كتابة الأمر:

Ex:1

```
router#show ip route
<text omitted>
D 192.168.32.0/26 [90/25789217] via 10.1.1.1
R 192.168.32.0/24 [120/4] via 10.1.1.2
O 192.168.32.0/19 [110/229840] via 10.1.1.3
```

نلاحظ أن الجملة الثانية والتي تم معرفتها عن طريق بروتوكول ال Rip تحتوي على ال subnet mask يساوي 24 وهو مساو لـ ال default subnet mask للفئة "C" والذي يساوي 24، ونفس الأمر بالنسبة للجملة الثالثة والتي تم معرفتها عن طريق بروتوكول ال OSPF فهي تحتوي على ال subnet mask يساوي 19/ وهو أقل من ال default subnet mask للفئة "C".

وعلى ذلك يمكن تحديد أنواع ال Routes التي تنتمي للمستوى الأول Level One على الشكل التالي:

Default Route: والذي يرمز إليه بالعنوان 0.0.0.0 وال subnet mask 0/mask.

Supernet Route: وهو ال Route الذي يحتوي على ال subnet mask أقل من ال default subnet mask فمثلاً:

الشبكات من 192.168.0.0/24 إلى 192.168.255.0/24 يمكن عمل ال summarization لها لتصبح 192.168.0.0/16.

وعلى سبيل المثال، الجملة الأولى توضح هذه النقطة:

Ex:2

```
RouterB#show ip route
<text omitted>
C 192.168.0.0/16 is directly connected, Serial0/0
S* 0.0.0.0/0 is directly connected, Serial0
```

Network Route: وهو ال Route العادي الذي يحتوي على ال Subnet Mask مساو لـ ال default subnet mask على سبيل المثال:

الجملة الثانية في المثال التالي توضح ذلك.

Ex:3

```
router#show ip route
<text omitted>
D 192.168.32.0/26 [90/25789217] via 10.1.1.1
R 192.168.32.0/24 [120/4] via 10.1.1.2
O 192.168.32.0/19 [110/229840] via 10.1.1.3
```

وال Routes في المستوى الأول Level One إذا كانت تحتوي علي: Exit Interface أو Next Hop Ip Address في هذه الحالة تسمى ال Ultimate Routes، فمثلاً المثال الثاني الجملة الأولى تحتوي على ال exit Interface وبالتالي يعتبر ال Ultimate Route.

وقبل أن نأخذ مثال علي ذلك يجب الإشارة إلي شئ هام جداً:

أن بروتوكول الـ EIGRP الوضع الافتراضي فيه هو الـ Default هو الـ Auto Summary ومع وصول أول Update لشبكة معينة عن طريق الـ EIGRP يؤدي ذلك إلي تكوين الـ NULL0 INTERFACE وهذا الـ Interface يكون Match لأي Packet لا يعرف الراوتر Route لها وطبيعة هذا الـ Interface أنه يستقبل الـ Packets ويعمل لها Discard وهو أشبه ما يكون بالثقب السوداء في الفضاء.

وهذا يؤدي إلي عدم استخدام الـ Less Match ولا الـ Default Route في حالة الـ Classless Behaviour، لذلك يجب تعطيل خاصية الـ Auto Summary في الـ EIGRP.

ولنأخذ مثال لتوضيح هذه العملية بإذن الله:

إذا ووصل الراوتر Packet تريد الوصول إلى 172.16.1.130

```
C# show ip route
```

```
-output omitted-
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
S 172.16.0.0/13 is directly connected, FastEthernet0/0
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R 172.16.0.0/24 [120/3] via 172.16.1.1, 00:00:03, FastEthernet0/0
C 172.16.1.0/25 is directly connected, FastEthernet0/0
  172.17.0.0/25 is subnetted, 1 subnets
C 172.17.1.0 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 is directly connected, FastEthernet0/0
C#
```

هنا يبدأ الراوتر بالبحث في المستوى الأول فلا يجد Match هنا ينتقل للبحث في الـ Parent فيجد أن 172.16.0.0/16 مطابق فيبدأ بالبحث في المستوى الثاني ولكنه أيضاً لا يجد Match إذاً:

قد يقول البعض انه قد يأخذ 172.16.1.0/25 بالطلع هذا الكلام يحتاج إلي تدقيق، فلو نظرنا إلي الـ Subnet Mask للـ Route نجد أن الـ factor هنا يساوي 28 وبالتالي فإن الشبكة تنتهي بالـ Host الذي يأخذ العنوان 172.16.1.126.

هنا إذا كان الـ Classful Behaviour هو الـ default على الراوتر يقوم الراوتر بعمل Drop للـ Packet.

أما إذا كان الـ Classless Behaviour هو الـ default على الراوتر يقوم الراوتر بإعادة البحث ولكن هذه المرة يبحث عن Less Match فيجد أن S 172.16.0.0/13 مطابق فيقوم بإرسال الـ Packet من الـ FastEthernet0/0، وهنا لا يضطر لاستخدام الـ Default Static Route إلا في حالة لم يجد Less Match. وفي ختام هذه المقالة أسأل الله عز وجل أن ينفع بها.

```
RouterC#show ip route
```

```
<text omitted>
```

```
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
```

```
C 172.16.4.0/24 is directly connected, FastEthernet0
```

```
S 172.16.0.0/16 is directly connected, Serial0
```

```
C 192.168.1.0/24 is directly connected, Serial0
```

إذن كيف يبحث الـ Router في هذه المستويات -الأول والثاني- وكيف يحدد الجهة التي سوف يرسل إليها البيانات وكيف يحدد أي مخرج سوف يرسل منه هذه البيانات وكيف يفاضل بين هذه الـ Routes ؟

حقيقة إن عملية البحث هذه يمكن تلخيصها في النقاط التالية إن شاء الله: -أبداً الراوتر بالبحث في الـ routes المستوى الأول بألوانها التي ذكرناها آنفاً، هنا نحن أمام حالتين:

أ- أنه يجد Match أي أنه وجد الـ Route له الـ Subnet Mask يساوي أو أكبر من الـ Subnet Mask الذي عنده في الـ Routes Table وهذا ما يسمى بالـ Longest Match، بعد ذلك يبحث في هذا الـ Route هل هو الـ Ultimate أي هل يحتوي علي الـ Exit Interface أو الـ Next Hop Ip Address، إذا كانت الإجابة نعم يقوم بإرسال الـ Packet باستخدام هذا الـ Route، إذا كانت الإجابة لا ينتقل إلي الحالة الثانية ب.

ب- إذا كان الـ Route ليس الـ Ultimate أو بمعنى آخر أن هذا الـ Route هو الـ Parent هنا يبدأ يبحث في الـ Routes المستوى الثاني وهي الـ Child إذا وجد Match هنا يقوم بإرسال الـ Packet باستخدام هذا الـ Route، إذا لم يجد Match؟ هنا ننتقل إلي النقطة الثانية.

2- إذا لم يجد الراوتر Match هنا تعتمد الخطوة التالية على: هل الراوتر يعتمد علي الـ Classful Behaviour أم هل يعتمد على الـ Classless Behaviour ؟

قبل الـ IOS 12.3 كان الـ default هو الـ Classful Behaviour والذي يعني أن الراوتر إذا لم يجد Match في المستوى الأول أو الثاني فإن لا يبحث في الـ Routes التي تكون الـ Less Match ولا حتي في الـ Default Route أما بداية من الـ IOS 12.3 فإن الـ default هو الـ Classful Behaviour ما يعني أن الراوتر إذا لم يجد Match في المستوى الأول أو الثاني فإن لا يبحث في الـ Routes التي تكون الـ Less Match ثم في الـ Default Route.

مع ملاحظة أن سواء كان الـ Behaviour :

Classful أو الـ Classless فإن هذا يتعلق بطريقة البحث داخل الـ Routing Table وليس له علاقة هل الـ Routing Protocol المستخدم هو الـ Classful أم الـ Classless.

## > Certification Practice Exams



"you a Cisco Certification" وبرائي الشخصي أرى هذا الأمر بأنه تصرف خاطئ من سيسكو والذي سوف ينعكس سلباً عليها وعلى مصداقية الشهادات بشكل عام وإن كانت الشهادات قد فقدت مصداقيتها من زمن بعيد وعلى ضوء المطمع الجديد لسيسكو سوف تصبح الشهادات للزبالة بعدما كانت للحائظ فقط

## وأخيراً أعلنت سيسكو الحرب على مهربي الأسئلة

بقلم: أيمن النعيمي

خبر جديد وصلني اليوم وهو إعلان سيسكو الحرب على مهربي الأسئلة مثل الـ Pass for sure والـ Test Inside والـ Actual Test والخ... لكن الحرب سوف تكون بشكل مختلف وعلى طريقة سيسكو التجارية التي تعودنا عليها دائماً ببساطة ولكي تثبت سيسكو أن برنامجها الامتحاني هو شيء تجاري بحت أعلنت سيسكو الحرب على مهربي الأسئلة لكن كيف؟ ببساطة سوف تقوم بنفسها بنشر وتهريب الأسئلة التي سوف تطرحها عليك في الامتحان من خلال أول منتج لها وخاص بشهادة سيسكو CCNA وتحت شعار "ake a CCNA PracticeT" Exam before the real exam" وقد وضعت سيسكو لهذا المنتج سعر 79,95 دولار وهو يتضمن أسئلة ومحاكيات ولابات وبنفس طريقة الامتحان ونفس الوقت أيضاً وقد أتاحت أيضاً تحليل للأجابة الصحيحة ولماذا تم اختيارها ولكي لا أكون ظالم فسوف أنشر أيضاً جملة صغيرة وضعتها سيسكو في آخر الصفحة والتي أشك بمصداقيته وهي

A" Cisco Certification Practice Exam will not earn



# بوابتك نحو احتراف عالم تحليل الشبكات

بقلم: عمر السويدي

فأنت هنا إما تضيف RIP أو OSPF

فالعلمية من الآخر... معروفة، ولها نظام (سيستم) معين تتبعه.

كذلك ما هي نسبة تعطل أجهزة الربط الشبكي من راوتر وسويتش؟

ليست نسبة كبيرة.

فلذلك كله ولغيره من الأسباب، يسود ظن بأن تركيب أجهزة الربط الشبكي لمرة واحدة وعمل صيانة دورية كافية لأن تعمل بإخلاص وبدون أعطال، لذلك هذا التخصص بات ليس في درجة قوية.

يأتي الآن في الصورة محلل نظم الشبكة أو خبير محلل نظم الشبكة.

هذا التخصص الذي أنا أطلق على متمرسه لقب الطبيب، ذلك لأنه هو من يحدد مشاكل الأعطال، هو من يحدد وهو من يقول هذه مشكلة من بالضبط، هل هي متعلقة بالشبكة، أو الخوادم أو بالبرمجة؟ هو من في الحقيقة الذي يضمن خدمة بحسب الـ SLA المتفق عليه.

إذا سوف نعطي اليوم تطبيقاً عملياً لهذا التخصص، حتى هذه نبذة بسيطة خفيفة حول البرنامج الشهير الويرشارك Wireshark وهو الآن من أشهر برامج تحليل الشبكة في العالم، وبنسبة تنزيل عالية شهرية أو سنوية.

هذا البرنامج كنبتة مختصرة، يقوم بلفظ نسخ لما يمر في الأسلاك الشبكية من رزم (packets)، بحيث تتمكن به من الإطلاع على ماذا يحصل الآن في الشبكة، مما يساهم في إظهار مناطق المشاكل عن طريق إظهار طرق عمل الأجهزة على الشبكة وطرق استجابتها.

نرجع إلى موضوع البحث الرئيسي ونوضحه بمثال: يتصل بك رئيسك في العمل وهو غاضب يكاد أن يخرج من الهاتف قائلاً: إن البرنامج الرئيس لا يعمل بشكل جيد وذلك لبطء في الشبكة، أصلحه بسرعة قبل أن يشكونا إلى مدير الشركة (أو الدائرة)

فكيف ستصرف؟!

وسأزيد نقطة مهمة وهي غالباً ما نقوم بها

هناك شيء آخر...

وهي مشكلتك الحقيقية بالنسبة لك، هي أنك كنت قبل الاتصال بدقائق تنظر في شاشة مراقب الشبكة الذي تستخدمه، وهو لا يظهر لك أي ارتفاع في المؤشرات، بل يكاد يقول لك إن هذا اليوم هو اليوم المثالي بالنسبة لك!!

تبداً بك رأسك، وبشراب الشاي بصورة أكبر، أصحابك في المكتب معك يعلمون أنك في ورطة، فيؤثرون السكوت ثم يفضلون تركك حتى لا يعطلونك عن حل المشكلة!

هل هذا الموقف يبدو مؤلماً؟!

لا تخف فقد مررت به (أو هو مر بي) مرات ومرات قبلاً.

دعني أقول لك: إن الجواب يكمن في تحليل نظم الشبكة. (Network analysis)

هو فن عجيب ليس بالصعب، لكنه بالتأكيد ليس بالسهل، ويتطلب مهارات عدة، من الممكن أن أفردها

كلنا نعرف وظيفة مهندس الشبكة، لكن كم منا من يعرف وظيفة محلل نظم الشبكة؟ من هو؟ ما هو عمله بالتحديد؟ ما درجة أهمية عمله؟ لماذا هذه الوظيفة موجودة بشكل نادر في عالمنا العربي؟ هذه الأسئلة أرجو أن أتمكن من الإجابة عليها في هذا المقال.

فنفقول بعد الاستعانة بالله سبحانه وتعالى...

مهندس الشبكة هو من يقوم ببرمجة الأجهزة المستخدمة في عمل الشبكة، فهو نوعاً ما مبرمج لكن ليس على البرامج المعروفة مثل البرمجة بلغة السيكيال والأوراكل وغيرها، فهو متخصص أكثر في برمجة خطوط وشبكات الاتصال.

نستطيع أن نتفق نوعاً ما على أنه يشبه مهندس الطرق.

هناك الكثير من التقنيات التي تستخدم في إنشاء الربط الإلكتروني، وكذلك هي تنقسم إذا ما كانت شبكة نطاق محلي (LAN) أو شبكة نطاق عريض (WAN)

يمر الطالب بمراحل عدة يتعلم فيها ماهية هذه الأجهزة التي تستخدم في إنشاء الربط الإلكتروني، كيف يتعامل معها، كيف يبرمجها، كيف يطلع على ما فيها من نظم، كيف يعمل لها ترقية،... إلى آخره. هذا الشخص الذي يعني بهذه الأمور يسمى مهندس شبكة أو مهندس نظم شبكة أو مهندس اتصالات الشبكة، وقد يطلق عليه أسماء أخرى.

وطريقة عمل مهندس الشبكة (سنستخدم هذا المسمى) في حالة حدوث مشكلة ما في الشبكة، أن يذهب إلى الجهاز الأقرب لمكان المشكلة، ويبدأ بالضغط على الأزرار للإطلاع على الأعطال الموجودة في الجهاز، أو يحاول استخراج الرسائل (syslogs) التي يرسلها الجهاز عن الأعطال الموجودة (في حالة قيام المهندس بعمل تفعيل لهذه الخاصية).

لكن دعني أسألك سؤالاً، كيف ستصرف إذا ما كان البطء ليس بسبب جهاز من أجهزة الشبكة، بل في بطء استجابة DHCP Server؟

كيف ستعرف أن هناك مشكلة إذا ما كان كل شيء يبدو طبيعياً لكن السبب في بطء مكان ما هو بسبب ضغط على وصلة الـ Backbone فقط.

كيف ستعلم أن البرنامج الرئيس المستخدم في مكان عملك قد تختلف استجابته إذا ما استخدم في شبكة النطاق العريض؟

إذن كيف ستتعرف على المشاكل الحقيقية وكيف ستضمن تقديم خدمة على مستوى عالٍ؟

هناك سوء فهم لهذا التخصص، أعني تخصص هندسة الشبكات، ذلك أن الكثير ممن يعملون في تقنية المعلومات يظنون الإدراك لهذا الفن، وفي الحقيقة للأسف يرجع غالب السبب في ذلك إلى مهندسي الشبكات أنفسهم، وسأوضحه بمثال.

قامت الشركة التي تعمل فيها بعمل فرع جديد.

في الغالب كل الذي سوف تعلمه سوف تضيف راوتر، وتعمل Static route ثم أضيف فرع آخر، وأنت كل الذي قمت به، طلب خط جديد للفرع الثاني، طلب وصلة Serial وإضافة Static route جديد.

بعد فترة صارت الأفرع كثيرة وصار هناك طلب على إمكانية وصول فرع إلى فرع آخر مثل البنوك،

في مقال في المستقبل، إن شاء الله تعالى،  
أرجع إلى السؤال الذي طرحته سابقاً

كيف تتصرف مع هذه الحالة ؟

في الحقيقة مع مر السنين، وجدت أن المشكلة الحقيقية ليست في وجود مشكلة مثل هذه، لكن في نقصان معرفة الشخص الطريقة في التعامل مع هذه الأنواع من المشاكل.

أعني.... يجب أن تجيب على سؤالي الذي طرحته هكذا،،،

في حالة استقبالي اتصالاً من هذا النوع، فيجب علي أولاً أن اتعرف إلى المشكلة عن قرب وكثب.

من الذي اشتكى؟ خذ رقمه، اتصل به،

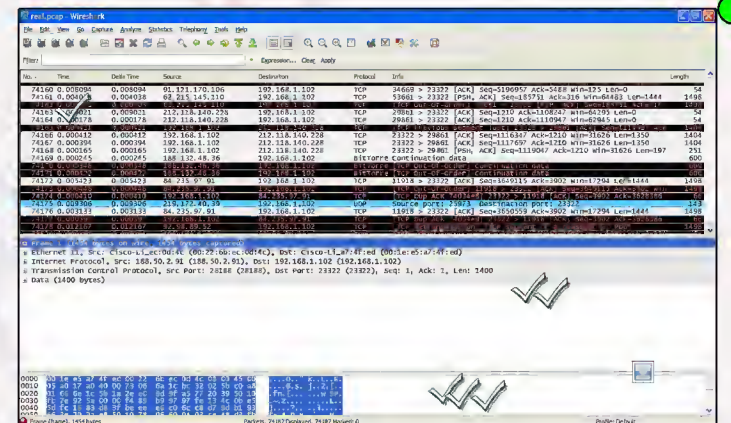
اعرف شكواه بالضبط، وقد يحتاج أن تذهب إليه.

لهكذا نوع من المشاكل، وجد ما يعرف بالواير شارك (Wireshark)، فهو برنامج لاقتطاع لكل ما يمر في الشبكة (حسب تجهيزك) يظهر لك محل الضعف إن وجد.

الآن.... لنقل إن المشكلة كانت فقط عند شخص واحد. حيث يعاني من بطء شديد في الوصول إلى قاعدة بيانات الأوراكل Oracle Database .

في الغالب سوف يكون هذا الشخص متصلاً بالشبكة عن طريق وصلة إلى Switch فاعمل Port mirroring إلى الواير شارك دع الواير شارك يعمل لفترة 15 دقيقة مثلاً، بشرط أن تطلب منه أن يعمل على البرنامج الذي يشكو منه، وبهذه الطريقة تلتقط كل ما يمر لذلك الشخص بالتحديد.

بعدها ستظهر لك شاشة مثل هذه:



كما هو ظاهر لك في الصورة، ستري الكثير من الألوان والكلام.

الآن... هل انتهيت إلى وجود علامات الصح؟

أولاً: أرغب في أن تعلم أن هذه هي صفحة الواير شارك الرئيسية عندما يكون في وضعية العمل، فهنا تتم دراسة الحالة التي تواجهك.

المكان الذي توجد به علامة صح واحدة، تستطيع أن تقول إن العمل كله يدور حول تفسير ما في هذه المنطقة، في الحقيقة كل ما في البرنامج ليس إلا شرح لما هو هنا.

هذا الجزء يحتوي على:

ترقيم للرمز (packets) التي استطاع الواير شارك أن يلتقطها وتوقيت ومرسل ومرسل إليه والبروتوكول المستخدم بينهما وقليلاً من المعلومات المهمة حول هذه الرزمة.

أما بالنسبة إلى المنطقة التي تحوي على نتيئين من علامات الصح، فهي شرح تفصيلي للرمزة التي أشرت إليها في المنطقة العلوية.

كما تعلمون في نظام البروتوكولات، بروتوكول يحوي خانات، فالمنطقة الثانية يتم فيها عرض هذه الخانات بطريقة سهلة ومقروءة، في هذه النقطة تستطيع أن تكتشف حتى التلاعب في أي بروتوكول.

أما بالنسبة للمنطقة التي تحوي علامات صح ثلاث، فهي منطقة hex، تستطيع أن تقول إن الكلام الحقيقي الذي انتقل عبر السلك في هذه المنطقة، وهي كذلك منطقة مهمة جداً، يهتم بها أكثر من يهتم أصحاب التخصصات الأمنية والهاكرز، حتى إنك تستطيع أن تجد الأرقام السرية هنا.

هذه كانت نبذة بسيطة عن واجهة البرنامج الرئيسية.

الآن تعرف إلى المحادثة التي كانت بين الزبون/الخادم (client\server)، بل إنك سوف تتمكن من عمل تصفية (فلتر) لتلك المحادثة بالتحديد، بحيث إنك ستتمكن من جعلها موجودة وحدها، فافعل ذلك. بعدها قم بعملية القراءة من البداية. تعرف هذه الأمور المهمة:

ما نوع البروتوكول المستخدم؟

ما نوع المنافذ (ports) المستخدمة بينهما؟

ما هي سرعة الاستجابة بينهما؟

من الأخطاء بينهما؟

انتبه إلى التلوين، فالتلوين له معان كثيرة تسهل عليك عملك.

أهم نقطة يجب أن تعلمها في هذا النوع من الأعمال.

ليس هناك حلاً واحداً دائماً للمشكلة التي تواجهك

أعني عندما افترضت المشكلة في المثال في هذا المقال، لاحظت أنني لم أعطك الحل، لم أقل المشكلة هي كذا وكذا.

وذلك لسبب!!

ذلك أن هذا النوع من الأعمال يتطلب تركيزاً شديداً، فأحياناً تواجهك مشكلة مرات عدة، لكن في كل مرة يكون الحل مختلفاً.

أعني.... أحياناً يبدو لك التشابه بين المشاكل لوجود نفس العوارض.

لكن (((صدقني))) في هذا النوع من الأعمال، تشابه الأعراض لكن لأسباب مختلفة.

فعند المثال المذكور هنا، قد تكون المشكلة، لوجود عطل في الـ (NIC) أو منذ في الـ (switch) أو السلك الشبكي له، أو لأن الحاسوب قديم وبه معلومات عن الشبكة قديمة مخزنة في مثلاً LMHOST. هل تصدق أن هذا من خلال تجربتي الشخصية!! وليس نقلاً عن أحد، وإلا كان كل شخص أعطاك أكثر.

كذلك يجب أن تعرف، ففي عالم الشبكات نحن نتكلم عن الثواني بالملي (mili seconds)... فالتخاطب بين الأجهزة يكون بالملي أو حتى أقل، وحدث تأخر في الاستجابة، يعني أن يصل التأخر في 50 ميلي وهذا يكفي لأن يكون هناك بطء..

على سبيل المثال، أنا أعرف أن Leased Line بسعة 2mb بين فرعين سوف يكون الوقت بين 9 ميلي ثانية إلى 20 ميلي ثانية، فكلما زاد 30 ميلي ثانية أتوقع حدوث نوع من البطء في الاتصال. فعندما أساعد في حل مشكلة في هذا الخط، أعرف أن في محيد 50 كيلو متر، فإن السرعة بهذا النوع سوف تكون من 9 إلى 20 ميلي ثانية، وإلا كانت هناك مشكلة.

الآن يجب أن تعلم أنه قد تختلف السرعات بحسب جودة الأسلاك المستخدمة، فمن الممكن في بلد ما تكون الخطوط من النوع المتوسط الجودة، إذا... يجب أن أتوقع توقيت مختلف. وهكذا..

إذا ما الطريقة في ضبط أمر التوقيت؟

أقول لك الطريقة هي التوثيق، والتوثيق فقط.

بمعنى... ابدأ بفحص الشبكة الداخلية أو الخارجية في أوقات مختلفة وأيام مختلفة لفترة من الزمن، وسجل الأرقام على ورقة معدة لهذه المهمة. كذلك ضع خانة بجانب هذه الأرقام، بحيث تسجل في هذه الخانة انطباعات المستخدمين لهذه الشبكة.

تستغرب!!!

دعني أقل لك شيئاً... من يعرف أن السرعة مثلاً 50 ميلي في الثانية في شركة من الشركات تعتبر لا بأس بها!

أليس من الممكن أن هذا يدخل في جودة الخط وأسعار شركات الاتصال!، فذلك شيء ممكن الحدوث!

إذا لا تستعجب

فأنت ترى بطلان لكنهم لا يعانون من مشكلة، فهم يعلمون أن الخط سوف يقوم بإعطائهم هذه الجودة، وهو راضون عن ذلك.

لذلك تسجيل انطباعات الموظف عمل مهم جداً.

الآن... بعد تسجيلك لتلك الملاحظات، وعند حدوث شكوى بسبب بطء شديد، سوف تشغل برنامج الواير شارك الخاص بك وتتركه يعمل لفترة معينة، وبعد ذلك تقوم بفحص النتائج ومقابلتها مع بعضها البعض، عندها ستتمكن على الأقل من تحديد المشكلة بشكل أسرع وأفضل، حتى تصل في النهاية إلى معرفة مصدر المشكلة.

حتى لا تكون قراءتك مجرد تسليية وتمضية وقت. لدي مهمة لك. تعرف إلى برنامج الواير شارك، حاول أن تتعامل معه، اطلع على قوائمته. اجعله مألوفاً بالنسبة لك. اكسر جدار الوحشة بينك وبينه.

حتى تمسك بأزمة هذا الفن تعلم الأمور التالية:

1- أنواع الـ protocols المستخدمة.

2- التوقيت

3- المحادثة بين الشخص والسرفر، لاحظ التوقيت في هذه المحادثة بالضبط.

4- تعلم إن شاء فلاتر

5- انظر إلى الـ Window Size

هذه كلها إن شاء الله يمر الوقت سوف أقوم بإفرادها جميعاً وغيرها بمواضيع متخصصة وماتعة.

ملاحظة مهمة جداً جداً...

لا بد أن تعلم أن هناك آثاراً مترتبة على استخدام برنامج لاقتطاع مثل الواير شارك، فقد لا يسمح لك عملك بعمل هذا النوع من الاختبارات لما ينطوي عليه من معرفة أسرار، خصوصاً لمن يعمل في المصارف، لذلك هذا كل لداعي التعليم وليس لمعاونتك على أي عمل غير قانوني.

باختصار...

هذا الدرس والدروس القادمة، إن شاء الله تعالى، لغرض التعليم فقط، ونحن نخلي أنفسنا من أي مسؤولية قانونية لما قد يترتب نتيجة استخدام البرنامج بطريقة غير قانونية.

عمر السويدي

Om18899@gmail.com

### فن تحليل نظم الشبكة فن علمي عملي ###



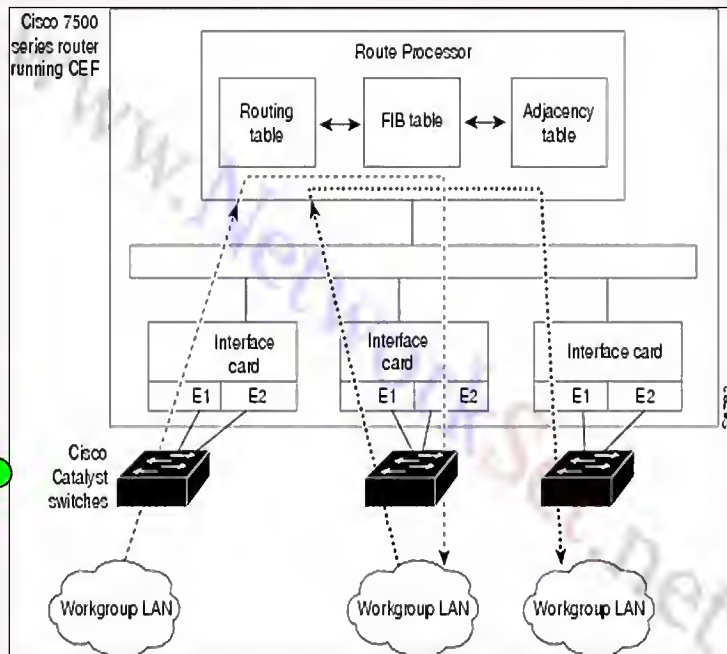
FIB أو Forwarding Information Base وهي نسخة طبق الأصل من Routing table والجدول الثاني يدعى Adjacency table وهو أيضا طبق الأصل من الـ ARP table وسوف نستنتج من كل ما ذكر بأن الموضوع فارغ حتى الآن وقد عدنا إلى نقطة البداية وكل ما ذكره اقتصر على نسخ جداول وتغيير أسمها فقط لذا لندخل في فوائد هذه التقنية

### فوائد تقنية الـ CEF ؟

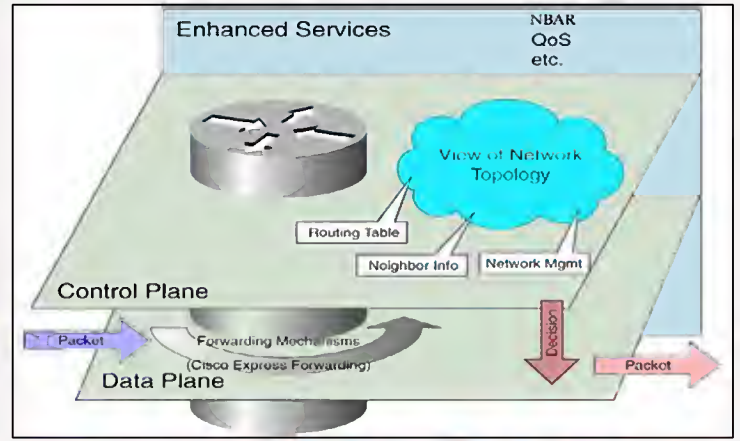
لنتفق أولا على شيء مهم أن الأداء والمرونة لن تلاحظهم في الشبكات الصغيرة لأن هذه التقنية هي موجهة للشركات الكبيرة والأنترنت لذا ضع هذه النقطة نصب عينك ولننتكلم عن الفائدة الأولى وهي

**الأداء والسرعة :** بعد ذكرنا لموضوع نسخ الجداول أستنتجنا أن هذه التقنية لم تقم بأي شيء جديد وهذا كان أستنتاج خاطئ والتفسير هو كالاتي عندما يطرأ أي تغيير على الـ Routing table فأول شيء يقوم به هو إعادة بناء الجدول من جديد وهذا سوف ينعكس أيضا على الجدول الخاص بي الـ Route-cache ومن هذه النقطة أخذت هذه التقنية فكرت نسخ جدول الـ Routing إلى جدول آخر وهو الـ FIB لأن أي تغيير سوف يطرأ هناك سوف يصل للـ FIB كتحديث بسيط على الجدول وبالتالي لن يتم إعادة بناء الـ Route-cache وهذا كله سوف ينعكس على أداء المعالج الخاص بالروتربالضافة إلى سرعة أكبر من الـ Fast Switching.

**Scalability** وللأسف لا يوجد له معنى في العربي ولكن فهم هذه الفائدة يتطلب منك فهم الوضعيات الموجودة في الـ CEF وهما وضعيتان: **الأولى** Central CEF وفيها يتم وضع ومعالجة الـ FIB و Adj في الـ Route process بشكل مباشر وهذه صورة توضيحية للوضعيات الأولى والذي يتضح من خلالها أن تعامل كل المنافذ يتم مع الـ Route Process



أما الوضعيات **الثانية** والتي يطلق عليها Distributed CEF فهي مخصصة لأنواع قليلة من الأجهزة وهي على حد علمي موجودة في روترات series 12000 وسويتشات 6500 أما عن آلية عملها والتي تشرح الفائدة الثانية في الـ CEF فهي تتركز في عمل نسخة للـ CEF table ووضعها على كل Line Cards وبالتالي سوف يكون لكل الـ Card أو الـ Interface الجدول الخاصة به وسوف يعمل بشكل منفصل عن الآخرين وبالتالي تعاملنا مع كل منفذ على حدى وأمنا له الجداول الخاصة به وبشكل مصغر عن الجداول الكبيرة والتي تحوي خيارات أكثر والذي ينعكس إيجابيا على سرعة إيجاد أفضل مسار والصورة القادمة سوف توضح كل شيء



## ماهي تقنية الـ CEF وكيف تعمل

بقلم: أيمن النعيمي

CEF أو Cisco Express Forwarding وهي كما يتضح أنه أحد التقنيات التي قامت سيسكو بتطويرها لكي تعطي سرعة وأداء أكبر في نقل البيانات على الروترات أو أفضل أن أقول الأجهزة التي تعمل على الالايير 3 بالإضافة إلى تفعيل خواص إضافية في الروتر مثل الخاصية الرائعة من سيسكو NBAR

### مقدمة هامة

لكي نفهم هذه التقنية يجب علينا أن نفهم بعض الأشياء حول كيفية عمل الروتر بشكل عام وأول الأشياء التي يجب أن نفهمها هو مصطلح Switching يطلق هذا المصطلح على التقنية التي تقوم بتوجيه الـ Packet إلى المسار الصحيح ومن هنا أحب أن أذكر بأن لا تخط الأمور بين الـ Switching الموجود على الطبقة الثانية وبين الـ Switching Packet الخاص بالروتر فهما شيان مختلفان جداً نعود إلى موضوعنا وهو كيف يعمل الروتر؟، ليقوم الروتر بتمرير الباكيث يجب أن يقوم بخطواتان مهمتان :

**الأولى** Make a routing decision for the packet اعتمادا على معلومات الـ Network Topology والتي يقوم الـ Routing Protocol بتوضيحها من خلال الـ routing table بالإضافة إلى مراجعة البولييسي الموجودة على الروتر وأقصد بهذه الكلمة الأكسس ليست و الـ Policy-based routing (PBR) والخ...وهي تستخدم جميعا من أجل تحديد المكان الذي يجب إرسال الباكيث إليه

**الثانية** Switch the packet وهي تتضمن نقل الباكيث من الـ Input buffer إلى الـ output buffer وإعادة كتابة الماك أدريس الخاص بي الـ Next-hop ومن هنا نستطيع أن نستنتج أن الروتر يحتفظ بهذه العناوين في مكان مخصص يدعى الـ ARP table والتي يتم تسجيل فيه الأيبي والمالك أدريس المطابق له.

ولهذه العملية (Switching) ثلاث mechanism مختلفة والدعمومة من أجهزة سيسكو وهي :

Process switching  
Fast switching (default)  
Cisco express forwarding (CEF)

سوف لن أتحدث عن أول اثنتان لأن الموضوع سوف يطول ولأن الموضوع من الناحية النظرية بسيط نوعا ما وقد تعرفنا عليهم في أبسط كورسات الشبكة لكن أحب أن أؤنوه إلى شيء مهم وهو الـ Fast Switching هي التقنية التي تعمل في الوضع الطبيعي على أجهزة سيسكو ولنبدأ حديثنا حول تقنية الـ CEF

### ماهي تقنية الـ CEF وكيف تعمل ؟

كما أتفقنا بأن الـ CEF هي عبارة عن Switching technology خاصة بسيسكو وأجهزتها فقط وأول ماتقوم به هو عمل جدولان خاصان بها الأول يدعى

والفائدة الثالثة هي إتاحة مميزات كثيرة للروتات مثل ميزة الـ NBAR و Cisco AutoQoS و Based frame relay traffic shaping (FRTS) و CEF لن تعمل كل هذه الخواص والنقطة الأخيرة التي سوف أختتم فيها حديثي وهي طريقة تفعيل الخاصية وهي من أسهل الأشياء التي تراها في سيسكو وتتم من خلال امر واحد

Cisco's IOS

Router(config)# ip cef

وهذه بعض الأوامر التي تستخدم في التبريل شووت

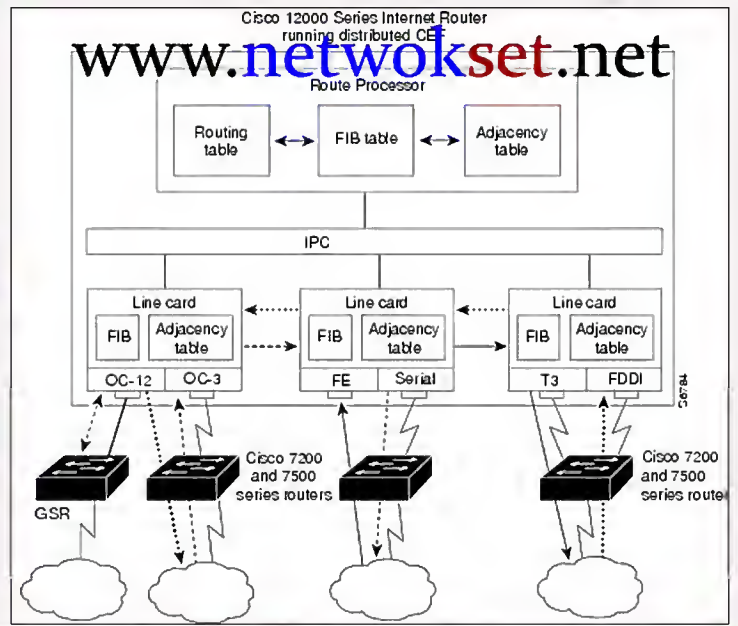
Cisco's IOS

Router#show ip cef

Router#show ip cef summary

Router#show ip cef detail

Router#show adjacency



# شهادة الـ CCIE تجربة-نصائح-ملاحظات

أعداد: عدنان بن خالد الشمري

cisco press and cisco learning مع CCNP Academy فقامت بعملها جميعها مرة واثنين وثلاث مرات وطبعاً كنت أستخدم dynamips then GNS3 واجه مشاكل في عملي السويتشات فكنتم أستخدم لابات موجودة في العمل عندي ثم بعد ذلك أصبحت أحمل لابات من موقع سيسكو زانفاندا عندي ثم أخيراً أخذت من أحد أصدقائي لابات IPExpert with dynamips files including initial configuratio ثم بدأت أطبق عملي كل هذه اللابات وكانت تعتبر نقلة كبيرة في زيادة معرفتي وخبرتي بخفايا هذه التكنولوجيا وكنت سعيد بذلك بعد ذلك جأت مرحلة المعهد (معهد آباد) وسجلت فيه للاستفادة بخبرة الناس الموجودة وخاصة ديفيد في كيفية التعامل مع الاختبار والاستفادة من روح فريق العمل وبدائنا نعمل سوياً ونحل السيناريوهات ونتناقش في الحلول والاستفادة من اللاب العملي الموجود بالمعهد وان كان فيه بعض المشاكل لكن كنا دائماً نجد حلول سحرية لأي مشكلة تقابلنا وتم الاعداد حتي المحاولة الأولى للاختبار لمدة 4 شهور وطبعاً في خلال هذه المدة أخذت من أحد أصدقائي جميع المواد الخاصة بالامتحان من (internet network expert) وهذه المواد صراحة فوق الممتازة وتعطي معلومات وخبرة غير عادية فطبعاً ذكرت هذه الكتب واللابات وحلول المشاكل فيها كمية تدريبات غير عادة للاستفادة والحمد لله استغدت من بشكل رائع والحمد لله

س: 6: هل التطبيق على الديناميس كافٍ لو في حال لم يكن هناك إمكانيات لشراء أجهزة؟ وماهي الأشياء التي لا تدعمها المحاكيات؟ بالنسبة للتطبيق علي gns3, dynamips جميل جداً ومهم جداً جداً وفي متناول الجميع ولكن هذا ممتاز في حالة الروتينج ولكن في حالة السويتشنج بنسبة 60% جيدة لان معظم أوامر السويتشات لا تنفذ عليه وبالتالي لازم استخدام لاب حقيقي عملي ولو لمرتين في التدريب علي الأقل اذا فالتطبيق فقط علي الـ dynamips غير كافٍ .

س: 7: ماهي اسباب عدم النجاح أول مرة يعني ماهي المعوقات التي

صادفته وكانت السبب في الرسوب حتى يستفاد منها؟

بالنسبة للنجاح أو الرسوب هذا توفيق من عند الله عز وجل بس مما لا شك فيه كان هناك أخطاء فائتلة في المرة الأولى وتداركنا هذه الأخطاء بعد ذلك والناس بدأت تنجح والمرة الثانية كان هناك مشكلة وكان السبب الرئيس فيها هو التأخير في الدفع لقبول الاختبار بوقت بسيط وبالتالي عندما ذهب لم أجِد اسمي وحدثت لي بعض المشاكل التي أثرت عليا ولكن الحمد لله ووقفت في المرة الثالثة بفضل الله عز وجل لكن أنصح دائماً بحجز الاختبار قبل الميعاد علي الأقل 15 يوم والتأني والتركيز وفترات ما بين السطور في الاختبار وهذا أمر مهم جداً كي لا تحل السؤال بشكل غير مطلوب وبالتالي النتيجة ستكون غير جيدة

أنصح أيضاً بالتركيز والتدريب المستمر علي مسائل troubleshooting حل كثير وتدريب كثيراً فالحمد لله من كثرة تدريبي حلّيت الـ trouble ticket في واحد ساعة وفورت ساعة للسياريو في الاختبار

س: 8: كيف توفيق بين الدراسة والعمل والظروف الاجتماعية؟

هي فعلاً معاناه وخصوصاً للمتزوجين ولديهم أسرة ولكن الحمد لله استطعت التوفيق بتشجيع أهلي

حروف اسم هذه الشهادة هي اختصار للجملة Cisco Certified Internetwork Expert تعتبر شهادة CCIE هي قمة الهرم بالنسبة لشهادات سيسكو، بل إنها تتعدى ذلك حيث تعتبر الأعلى علي الإطلاق بين جميع شهادات تكنولوجيا المعلومات وهندسة الشبكات، ومبدأ سيسكو فيها لا يكفي أن تعرف، بل يجب أن تعرف كيف تطبق ما تعرف . لا توجد شروط أو متطلبات لنيل هذه الشهادة وأيضاً لا تشترط سيسكو الحصول علي CCNA ولا CCNP ولا غيره. فبالإمكان التقدم لنيل هذه الشهادة ( مباشرة ) هذا بالطبع لن يجرؤ ولديه ثقة تامة في قدراته ( ولكن من الضروري أن يكون لديه كافي بمناهج هذه الامتحانات لأن CCIE هي تجميع لكل ماورد فيها. ويكفي أن نعرف انه منذ أن أطلقت سيسكو هذه الشهادة في 1993 لم يتعدى عدد الحاصلين عليها 20000 لا منذ فترة وجيزة فقط، مقارنة بمئات الآلاف أو حتى الملايين الحاصلين علي شهادات سيسكو غيرها. ومن المعروف أيضاً إن نسبة النجاح في هذا الاختبار من أول محاولة تكاد تكون شبه مستحيلة ولكن لا يوجد مستحيل مع الإصرار والمثابرة. لذلك نتمنى من الكل الحصول عليها بجد وجهد وجداره ولقد أجرينا مقابلة مع أحد المهندسين الحاصلين حديثاً علي شهادة CCIE وهو المهندس هاني إبراهيم إليكم هذه المقابلة وإن شاء الله تكون عند حسن ظنكم وتستفيدوا من خبرات غيركم .



س: 1: من هو هاني إبراهيم؟  
هاني إبراهيم مهندس شبكات بشركة أول نت متخرج من كلية الهندسة جامعة المنصورة تخصص اتصالات

س: 2: كيف كانت بدايتك مع دراسة الشبكات؟

لقد بدأت بالعمل كمدرّب للشبكات وكنت وقتها هنا في السعودية وادرس دبلوم الشبكات سنه وستين حتي جاء لي صديق سعودي وقال لي انه يدرس سيسكو أكاديمي في مهدع الخليج ويريد

ويريد مساعدتي فوافقت ودرست له المنهج كاملاً وعقب انتهاء المنهج تقدمت باختبار CCNA ووقفت الحمد لله وأنا مازلت أتذكر نتيجة الاختبار هو 896 وبدون وجود dumps وقتها مثلما هو الآن

س: 3: ماهي الشهادات والدورات التي حصلت عليها ؟  
بترتيب الأقدمية

CCNA, A+, MCSA, CCNP, MPLS (CCIP), CCSP  
And at last CCIE LAB V4

س: 4: ماهي الصعوبات التي وجهتك خلال الحصول على الدورات وشهاداتها؟

- الوقت الكافي للمذاكرة حيث إنني كنت أعمل دوامين

- الانفاق المادي علي الاختبارات والكتب

- قلة التطبيق العملي وان كنت تغلبت عليها باستخدام dynamips, gns3 في سيسكو , virtual machine مع ميكرو سوفت

س: 5: كيفية التحضير للامتحان CCIE وماهي الكتب والمناهج والابيات التي درست منها؟

- بداية أول شئ قمت للتحضير للاختبار إنني قمت بمراجعة منهج CCNP كاملاً من خلال



طبعاً الدراسة بشكل جيد والفهم الجيد للتكنولوجيا الموجودة والاستعانة بالخبرات التي سبقتنا في هذا المجال لكي نكون علي الطريق الصحيح مع التركيز طبعاً علي التدريب العملي مرات ومرات

س: 14 كيف كانت تجربتك في اختبار CCIE منذ البدايه حتى الحصول عليه؟

الحمد لله علي كل شئ انا دخلت مرتين ورسبت فيهم ومع التصميم وعدم اليأس وتشجيع اصدقائي لخاصة ديفيد وحزمة دخلت المرة الثالثة ووفقت والحمد لله

س: 15 ما هي البرامج والأدوات التي ساعدتك في الابات العملي، علماً ان البعض ليس عندهم معامل لذلك؟

طبعاً GNS3, DYNAMIPS بالإضافة طبعاً الي الالاب العملي الموجودة بالمعاهد

س: 16 اين درست CCIE؟

درست بمعهد أباد بالرياض

س: 17 لماذا معهد أباد؟

لان معهد أباد هو الوحيد الذي وجدته يقدم الالاب الخاص ب CCIE هنا في مدينة الرياض

س: 18 ماذا يميز معهد أباد عن باقي المعهد؟

أهم ما يميز معهد أباد صراحة هو فريق العمل به سواء إدارة المعهد او المدرسين فصراحة هؤلاء الناس متعاونين بشكل عالي جدا ولا نحس أبدا أننا طلاب بلا مشاركين في فريق عمل وورشة عمل من أجل الاستفادة والإفادة للجميع وللعلم هذه أول مرة اذهب لمعهد وادرس فانا دائما اعتمد علي الدراسة الذاتية.

كلمه أخيرة نقولها للقراء قراء مجله NETWORKSET؟

ارجو من الجميع التوكل علي الله واعمل ال عليك واجتهد والتوفيق من الله عزوجل ووفقنا الله جميعا لخدمة ديننا وأمتنا يارب العالمين

وفي الختام نبارك للمهندس هاني لحصوله على CCIE وانتظرونا مع مقابلات أخرى ,,,

لي وتفهمهم للوضع وتشجيعهم لي للحصول علي ما هو اكثر وبالتالي اعتقد انه لا يوجد مشاكل بعد ذلك والموضوع فقط محتاج مجهود وتعب للحصول علي ما تريد مع توفيق الله عز وجل

س: 9 ماذا تقول للذين ليس له القدرة المادية للحصول على دورات سيسكو ويريدون ان يبدعون في هذا المجال؟

والله المنتديات العربية في هذا المجال تقوم بدور جبار ورهيب في تعليم الطلبة العرب وانا في رأي انها تضاهي شركات التدريب العالمية بالإضافة الي أنها مميزة بالبساطة والموضوعية والوصول الي هدفها من أقرب الطرق - وهناك كم هائل من الكتب المجانية منتشرة علي النت لمن يريد المذاكرة وما هو افضل العملي اصبح عندك الآن gns3, dynamips فاهم شئ جمع العزيمة وتوكل علي الله وثق ان الله لن يضع تعبك ابدا

س: 10 ماذا تنصح إخوانك في المسار الصحيح للتعليم الصحيح في شهادات سيسكو لكي يتميز به؟

طبعاً بعد التوكل علي الله دائماً ثقي بنفسك وبقدراتك وانك ان شاء الله هاتخاذ هذه الشهادة وافهم جيداً محتوى المادة ويجب التطبيق العملي ثم التطبيق العملي ثم التطبيق العملي

س: 11 ما هي الكتب او المذكرات التي تنصح به؟

انا دائماً احب اذاكر من Cisco press , Cisco learning , CBT nuggets only for Jeremy

س: 12 كيف كانت دراستك او طريقتك في شهادة CCIE؟

بدأت طبعاً بمراجعة منهج CCNP كامل وعمل جميع الالابات الخاصة به ثم حصلت علي منهج INE شرح وعملي لعامي 2009 و2010 واهم حاجة فريق العمل الي كنت فيه مع المدرب ديفيد بمعهد أباد لاننا فعلاً اشتغلنا كثير واكتشفنا ما هو أكثر بروح التعاون ودعم الناس لنا بالمعهد

س: 13 ما هي الطريقة المثلى للابداع والتعلم في CCIE قبل الحصول على الشهادة؟

## أول شخص حصل على شهادة CCIE في العالم أكثر شخص حصل على شهادة CCIE في العالم

أعداد: أيمن النعيمي

Name	Certification Type	Certification Number	Track	Certification Status	Certification Date
CHANG MIN KIM	CCIE	12303	Routing and Switching	Re-certified	26-Sep-2003
CHANG MIN KIM	CCIE	12303	Service Provider	Re-certified	01-Sep-2005
CHANG MIN KIM	CCIE	12303	Security	Re-certified	02-Aug-2007
CHANG MIN KIM	CCIE	12303	Voice	Re-certified	21-Jan-2008
CHANG MIN KIM	CCIE	12303	CCIE Storage Networking	Re-certified	03-Jun-2010

بعد أن تعرفنا على أول شخص حصل على شهادة الـ CCIE لنتحدث عن أكثر شخص حصل على شهادات CCIE في العالم فالיום وبالصداقة وجدت على موقع learningnetwork الخاص بسيسكو على شخص كوري الأصل يحمل خمس شهادات من CCIE الموضحة بالصورة فوق وهو الآن في مرحلة التجهيز للشهادة السادسة الخاصة بالوايرليس

الشاب الكوري والذي اسمه Chang Min أتم الشهادة الخامسة من حوالي الثلاث أشهر فقط وقد تتفأجئ إذا أخبرتك بأنه بعد أربع أيام فقط من النجاح قد انضم لمجموعة لدراسة وتجهيز شهادة الـ CCIE Wireless وأخيراً أحب أن أشير إلى عمل صاحبنا الكوري وهو Computer Science and Engineering وسبب كتابتي عنه فقط من أجل أن تعلم يا أخي العزيز أن الوقت الذي لديك يساوي ذهب لكن أحياناً نسيئ تقديره وأعلم أيضاً أن مهما كان عمرك أن هناك دائماً وقت تستطيع ان تحقق فيه أكثر بكثير مما تحلم به فترتفع أنت ونحن وأمتنا إلى مستوى أعلى وأفضل مما نحن عليه لذا أخي العزيز أحرص دائماً على أن تتعلم كل يوم شيء جديد

ملاحظة صغيرة هدف المقال هو الإشارة إلى قيمة الوقت فقط وليس عدد الشهادات

سؤال بحثت عنه اليوم وهو من أول من حصل على شهادة الـ CCIE في العالم وأحببت أن أحدثكم عنه في هذه المقالة السريعة وقبل أن أخبركم من هو سوف أخبركم معلومة جديدة وهي أول رقم يبدأ في الـ CCIE ليس رقم واحد بل رقم 1024 وهي كانت رغبة سيسكو أي ربط الرقم بعالم الـ Binary 2^10 وقد حصل أول لآب مخصص لهذه الشهادة على الرقم 1024 وتم تعليق لوحة خاصة فيه في نفس الغرفة وهذه صورة لها



لنعد الآن إلى موضوعنا من هو أول من حصل على شهادة CCIE؟ أول من حصل على هذه الشهادة كان يحمل الرقم 1026 وكانت لي Terrance Slattery وسوف تلاحظ أن هناك رقم 1025 ليست لأول شخص والسبب كون هذا الرقم يعود لي الشخص الذي قام بأعداد وتجهيز هذا الأمتحان وهو Stuart Biggs لذا يكون Terrance Slattery أول شخص من أمتحن وحصل على هذه الشهادة في آب 1993 وهذه صورة له



Terry Slattery كان من أحد الأشخاص الذين قدموا الكثير لسيكو على مستوى CLI devel-opment, consulting, and training وقد تركها عام 2000 وقام بتأسيس شركته الخاصة Netcordia الخاصة ببرمجيات الشبكة <http://www.infoblox.com> وأخيراً لا يسعني إلا أن أتمنى للجميع بالتوفيق والحصول على رقم من هذه الشهادة

# من أين أبدأ وكيف أبدأ في الشبكات ؟؟؟

## سؤال لطالما حيرني !!!

بقللم: عادل الحميدي



نصائح للسنة الثالثة (نصائح متقدمة) : وفي الحقيقة هي كثيرة ولنعطي لذلك أمثلة/  
 المثال الأول: في سيسكو لدينا ثلاث اتجاهات هي المستقبل وهي:  
 VoIP تقنية الصوت عبر الإنترنت ، Wireless الشبكات اللاسلكية ،  
 Security الأمن والأمان في الشبكات ...  
 المثال الثاني: في مايكروسوفت عندنا اتجاهات كثيرة فموضوع الـ SharePoint  
 وموضوع الـ IP v6 ...  
 المثال الثالث: وبإسلام عليك لو تستطيع تذاكر كورسات لشركات منافسة في نفس  
 تخصص الشبكات لكن لشركات أخرى غير سيسكو ومايكروسوفت مثل/



منافس لـ سيسكو: جونيبر Juniper والتي تعتبر الآن صاحبة المركز الثاني فهي  
 ثاني أكبر شركات العالم المتخصصة في الشبكات حيث لها كورسات مثل JNCIA-ER  
 و JNCIA-EX و JNCIS-ER ثم المستوى الثاني JNCIS-SEC ...



منافس لـ مايكروسوفت: أنظمة التشغيل لينكس CompTIA و Linux و Sun  
 Certified SCOSA10S أو تلك Mac OS X Certification  
 وعندئذ أنت تستطيع بعدها أن تخرج من حيز الاحترافية إلى الخبراء CCIE مثلاً

، والله أسأل أن يوفقني وإياكم لخدمة هذا الدين اللهم آمين .  
 أنت الآن شخص تفخر بنفسك ويفخر بك كل من حولك ، تتقاتل عليك الشركات  
 مرتاح في عملك وراتبك كبير (راتب 60 ألف قليل عليك يا جهبذ) وحياتك سعيدة  
 فمن زرع حصداً وعندها لن تجني إلا الورد .

ثلاث سنوات يا أفاضل لا شيء في عمر الإنسان  
 ثلاث سنوات من العرق والدم ترتاح بعدها عمرك كله

أما بخصوص سيرتك الذاتية وكيف تسوق نفسك لم أجد أفضل من المواضيع المشتهة  
 في عرب هاردوير في قسم خدمات التوظيف والخاصة بالسيرة الذاتية على الرابط

التالي (أرجو منك أن تقرأها بتمعن وتحاول الاستفادة منها)  
<http://www.arabhardware.net/forum/forumdisplay.php?f=126>

كما يتوجب عليك الاشتراك في مواقع التوظيف والتقدم للوظائف من خلالها مثل/  
[www.bayt.com](http://www.bayt.com)

من أكبر مواقع التوظيف في الشرق الأوسط ، وغيرها كثير من تلك المواقع التي يجب  
 أن تكون حريص على الاشتراك بها ...

# إلى اللقاء في الحلقة القادمة #

تقرأون في هذه الحلقة ...

- 1) A+, N+, CCNA, MCP, MCSA, CCNP -> Cisco Certified ...
- 2) A+, N+, MCP, MCSA, CCNA, MCSE -> Microsoft Certified

نهاية الجزء الأول من المشوار سنتين من الثلاث سنوات ...

كورسات إضافية للمحترفين ...

انتظرونا في الجزء الثاني من حلقات:

من أين أبدأ وكيف أبدأ في الشبكات ؟؟؟ سؤال لطالما حيرني !!!

أبدأ مقال اليوم بالتهنئة بالعيد فأقول تقبل الله منا ومنكم صالح الأعمال وكل عام  
 وأنت من الله أقرب وعن عذابه أبعد ، ثم ألخص ما تم الاتفاق عليه حتى الآن تحت  
 عنوان :

خلاصة القول أنك مخير بين مسارين لتسير فيهما :

- 1) A+, N+, CCNA, MCP, MCSA, CCNP -> Cisco Certified
- 2) A+, N+, MCP, MCSA, CCNA, MCSE -> Microsoft Certified

وتفسيرهما كالآتي:

كلا المسارين نبدأ فيهما بـ A+ ثم N+ ... ثم

أولاً : مسار سيسكو / نبدأ فيه بـ CCNA ستكون عندها معقول ومقبول في  
 سيسكو وقبل أن تكمل المشوار ، ستحتاج لكي تغطي نقاط الضعف عندك في أنظمة  
 التشغيل أن تكون على دراية بالكورسات الأربعة الأولى من مايكروسوفت (في  
 اعتقادي ذلك ضروري) MCP ثم MCSA ، ثم بعدها ترجع لكورسات سيسكو  
 CCNP وتكمل المشوار في سيسكو كما سنوضح حالاً ...

ثانياً : مسار مايكروسوفت / نبدأ فيه بـ MCP ثم MCSA ستكون عندها  
 معقول ومقبول في مايكروسوفت وقبل أن تكمل المشوار ، قد تحتاج لكورس  
 CCNA (من سيسكو) في اعتقادي هذا اختياري ، ثم بعدها ترجع لكورسات  
 مايكروسوفت MCSE وتكمل في مايكروسوفت المشوار كما سنوضح حالاً ...  
 والآن أرجو أن تكون الصورة واضحة ...



والآن ملاحظاتي على المدة الزمنية :

1) Cisco: 3years (36month) - 13m(A+) + 3m(N+) + 2m(CCNA) + 1m(MCP) + 3m(MCSA) + 6m(CCNP) = 36 - 18 - 18 month.

2) Microsoft: 3years (36month) - 13m(A+) + 3m(N+) + 1m(MCP) + 3m(MCSA) + 2m(CCNA) + 3m(MCSE) = 36 - 15 - 21 month.

دعنا نتفق على أن هذه المدة مثالية نوعاً ما ، لأن الإنسان تقابله ظروف تسبب له  
 بعض التأخر لا أقول تعيقه فصاحب الهدف والذي لديه همة عالية لا يعيقه شيء ،  
 ولكن أقول هذا من باب الواقعية لذا سأقول أن تلك الكورسات حتى الآن استغرقت  
 من مدة الثلاث سنوات سنتين ...

لذا فقد بقي لنا سنة فإماذا نفعل في هذه السنة ؟؟؟

الآن وبعد أن حصلت على كل هذه الشهادات أعتقد أنك ستكون قادر على اختيار  
 طريقك بنفسك ولكنني لن أخجل عليك ببعض النصائح فكن معي ، ولكن قبل أن أبدأ  
 في سرد بعض تلك النصائح أريد أن نتفق على ما يلي ...

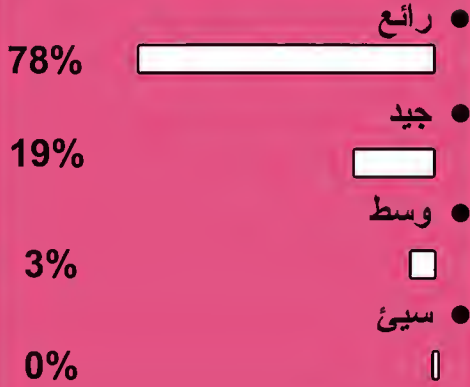
في الحقيقة أنا أريد هنا أن أسمى ما فات من مقالات بالجزء الأول من المشوار والذي  
 سأنهيته الآن ، لأبدأ فيه من جديد نعم مرة أخرى لكن مع التفاصيل المملة عن كل  
 جزء أو كورس وسأسميه الجزء الثاني من المشوار أرجو أن تكون الأمور واضحة ...  
 فالجزء الثاني سيكون شرح تفصيلي للجزء الأول من المقالات والله المستعان ، حيث  
 ربما نستمر في شرح تفاصيل عن كل كورس اتفقنا على أخذه حلقة أو أكثر حسب  
 الكورس والله الموفق ...



# نتائج الاستفتاء الشهري

## نتائج الاستفتاء

ماهو تقييمك للمجلة ومحتواها ؟



الاستفتاء الذي قمت به هذا الشهر كان هام جدا بالنسبة للمجلة فلقد أردت من خلاله تحديد مستقبل المجلة وقد طرحت فيه أربع تقييمات حول تقييمك لمستوى المجلة وللمحتوى وكانت النتائج صراحة غير متوقعة إلى هذا الحد فمع حوالي 250 صوت فقط كانت النسبة الأكبر منها في صالح الخيار الأول وهو رائع وحقيقة أردت من هذا الاستطلاع معرفة الآراء الأخرى للمجلة فانا أراها جيدة ومناسبة جدا كمحتوى عربي لكن أردت أن أسمع الطرف الآخر وهو أنتم والحمد لله حصلنا على تقييم رائع ومناسب جدا للمواصلة في المجلة ولا أخفيكم أيضا أن الرسائل التي تصلني كل شهر للمواصلة في هذه المجلة كافية لتحفيزي على مواصلة المجلة وفي نفس الوقت تخرجني بعض الشيء لاني الآن قد أكون قادر على المواصلة وتقديم الأعداد بشكل دوري وكل شهر لكن لا أعلم شيئا عن المستقبل وعن الظروف التي سوف تواجهني لذا أعود وأكرر طلبي من كل شخص قادر على كتابة أي موضوع يخص الشبكات أن يرسله لي لتقديمه للمجلة والذي يساعدنا على المواصلة في المجلة لذا الحل دائما هو معكم فمعكم المجلة لن تقف أبدا ان شاء الله.

وأخيرا أحب أن أتوجه إلى بالشكر العميق لكل من شارك معنا في هذا الصرح الصغير ولو بالشكر فهي تعد أيضا محفز لنا على الاستمرار وطبعا الأساتذة الذين يتواصلون معي ويشاركونني المجلة بمقالاتهم الممتعة والمفيدة وآخرًا لا ننسونا نحن فريق عمل المجلة من دعواتكم فهي كل مانهدف إليه من هذه المجلة للانضمام لفريق المجلة والتواصل معي : [admin@networkset.net](mailto:admin@networkset.net)

# شجع هذا النوع من المجلات بوضع أعلاناتك هنا

# لينكس والشركات الكبرى

بقلم: أحمد بخيت



Juniper®  
NETWORKS



HUAWEI

CISCO SYSTEMS



**التعددية Redundancy:** من خلال هذه النقطة يمكن استغلالها من أكثر من جهة، اول جهة ان السيرفر لا قدر الله لو حصل اي عطل مفاجئ Drop او خروج من الخدمة لأي سبب م الاسباب فان سيرفر مجاور له Backup سوف يدخل مكانه ويحل كل هذه المشاكل الى ان يعود السيرفر الأول للعمل وهكذا تستطيع تقديم الخدمات مع بعض المصادقية لأنها على الأقل ستكون مضمونة الاستمرارية والاستقرار، لكن الجهة الأخرى هي امكانية استغلال هذه الخاصية وتقوم ببناء Cluster كامل خاص بك وتقوم بتوزيع ضغط الخدمات على السيرفرات كلها بدلاً من سيرفر واحد وهكذا نجد ان هذه الخدمات ستكون أكثر اعتمادية من ذي بدئ كما انه تستطيع زيادة عدد العملاء الكسفيديين من خدماتك بهذه الصورة.

طيب طالما ان كل هذه المميزات وأكثر فان سيسكو قد اتجهت تجاه اللينكس ليس بسبب السعر فقط حيث انه مجاني لكنه على العكس نجد ان سيسكو لما اختارت فانها قد اختارت نظام مدفوع لكنه أكثر هذه الأنظمة استقراراً، وهذا فان الخدمات التي تقدمها سيسكو مثل الفويس VOIP المعروف عنها انها تستهلك موارد من السيرفر لهذا فان سيسكو قد اختارت اللينكس، لكن لو تركنا موضوع سيسكو بما فيه مع اني اعتبره موضوع شيق وواضح للكل لكن الذي يحيرني صراحة هو موضوع جونيبر حيث انه اتجهنا ناحية شركة جونيبر سنجد ان جونيبر من البداية ونظام تشغيلها JunOS كله من الروتينج Routing والسويتشينج Switching والسيكيوريتي Security وهي تظل متمسكة بنظام تشغيل أقوى من اللينكس وهو اليونكس UNIX ومن المعروف ان نظام FreeBSD هذا ليس مستقرأ فقط مثل اللينكس لكنه مستقر 100 مرة او بإمكانك ان تقول حوالي 1000 مرة أكثر وعلى فكرة فان هذا النظام مجاني ومفتوح المصدر Open Source وكمان مشهور انه لا يستهلك موارد بالمقارنة مع اللينكس العادي الا انه غاية في الصعوبة ويأويله الشخص الذي يكون مسؤول عن شبكة بها مثل هذا السيرفر اذا كان هذا الشخص غير متمكن، ولهذا نجد ان سويتشات جونيبر مشهور عنها انها اسرع واعلى في الكفاءة وكذلك ينصح بها ان تكون في الكور نتورك Core Network هذا بغض النظر على ان الهارد ويبيير لجونيبر احدث بحوالي 20 عام من سيسكو على فكرة المعلومة دي مش متأكد منها.

وكذلك يوجد جزء يمكن يكون بعيد قليلاً عن الشبكات لكن يمكن ان يكون له علاقة بالطب أكثر منه او له علاقة بالتعاون بين الطب والاي تي IT وهذا اكيد ناتج عن حلول الشركات التي تحاول ان تقدمها للمستهلكين الخاصين بها، على العموم ما حدث انه بعض اصحابي قد عملوا كمهندسين صيانة اجهزة طبية و كان واحد فيهم كلمني ان بعض اجهزة الاشاعات المقطعية الان نظام تشغيلها هو يونكس حتى يضمن استقرار الجهاز، وكذلك الحال لأصحابي في المجال العسكري والجيش كله الآن أصبح يتغنى باللينكس اذ ان انظمة الرادارات وتعقب الطائرات أصبحت شبكية وكمان بتعامل مع اللينكس ولو هنتكلم عن كدا راح نقول هواوي Huawei لأن هذه الشركة لديها نشاط في كل المجالات المتعلقة بالشبكات والاتصالات تقريباً والصيني يكسب.

وأحب ان أقول انه الآن اعمل بشركة مهمة يحل الشبكات وتقريباً حوالي 70 بالمائة من هذه الحلول مبنية على اللينكس بطريقة أو بأخرى وكذلك الحال عند البحث عن افراد لشغل احد الوظائف بقسم Network Solutions لدى الشركة والذي اتشرف بان اكون مديراً له لا نبهت فقط عن اشخاص سيسكو وبس او جونيبر لكننا نحاول نجد رجالاً فداشياً يتعامل كذلك مع اللينكس وهذا اهم لأن مثل هذا الرجل يكون قادر أكثر من الشخص المهتم ببسيسكو انه يقدم حلول للشركة.

اتمنى اني اكون حاولت اظهر شئ من اهمية اللينكس في حياتنا وانصح كل شخص يبيدتي حياته او تحت التخرج انه يحاول بل لابد له ان يتعلم لينكس وكمان يحترفه وربنا يوقفه.

كل عام وانتم بخير

في البداية اود ان انوه ان هذا المقال قد كتب مرتين اول مرة بالعامية المصرية على اعتبار ان هذه اللغة اسهل ومتعارف عليها مع الغالبية من القراء، لكن وخضوعاً لرأي اخي الكريم أيمن قد اعدت كتابتها باللغة العربية آملاً ان تحوز اعجابكم باذن الله، وانني لم كتبت بالعامية المصرية لم يكن هدفي الا توصيل المعلومة باقل جهد ولكي تكون اقرب الى القارئ وكأنا نجلس معاً في جلسة سمر. اليوم باذن الله سوف نتحدث عن الشركات الكبرى والبرامج او الحلول التي تستطيع مثل هذه الشركات تقديمها سواء كانت هذه الحلول على مستوى الشركات الصغيرة SOHO او الشركات الكبرى او المتوسطة Enterprise وباذن الله سوف نأخذ كمثال لهذا الموضوع شركات كبرى في حلول الشبكات أمثال سيسكو وجونيبر على اعتبار ان اغلبنا على الأقل اذا لم يكن قد احتك بهذه الأنظمة فانه سيكون اكيد قد سمع عنها سواء للدراسة او من خلال الشركة التي يعمل بها تستخدم أحد حلول هذه الشركات.

اول شئ نتكلم عنه هو الشركات الكبرى لم تعتمد هذه الشركات في الكثير من حلولها على لينكس خاصة الحلول الكبيرة منها ؟؟؟، حلول كثيرة مثل سيسكو كول مانجر CUCM اذ ان شركة سيسكو كان الى الاصدار الثالث او الرابع تقريباً تعمل على منصة الويندوز سيرفر 2000 و 2003 لكن بعد هذا نجدهم قد تنهوا بلا رجعة اتجاهها كاملاً تجاه اللينكس وأكثر من ذلك نجدهم قد اختاروا توزيعاً تعتبر من اصعب التوزيعات Rough وهي توزيعة الريد هات RedHat ومن المعروف ان الريد هات من الاصدارات الغير مجانية في عالم اللينكس لكن ما يميزها يجعل العديد ينقض عليها ويعتمد عليها دون غيرها في كثير من الحلول وكذلك نجد ان الكثير من حلول مجال VOIP المجانية مثل سيرفر Asterisk قد تم بناؤه على توزيعة في الاصل هي ريد هات وهي سنطوس CentOS وكذلك العديد من سيرفرات الاضافة لكن الريد هات تتميز بعدة مميزات سنستعرض بعض منها وليس على سبيل الحصر:

**الاستقرارية Stability:** لينكس ريد هات مستقر لدرجة انك ممكن كل خمس اعوام فقط انك تزور غرفة الشبكات او السيرفرات لديك IT او الغرفة التي تحفظ بها الاجهزة Server Room وتقوم فقط بمسح التربة التي قد تراكمت على هذا السيرفر بلا اية مبالغة طالما لم تحدث اعطال باور Power Breakdown او اشيء قد تدمر الاجهزة الالكترونية عامة خاصة بالكهرباء.

**الدعم الفني Technical Support:** من المؤكد لدينا انه عند شرائك جهاز معين غالي جداً بالمقارنة مع ما يساويه من اجهزة لشركات منافسة اخرى فان وراء هذا الارتفاع في السعر خدمات أخرى تستطيع الحصول عليها بعد شراء هذا الجهاز حيث انه مع توافر خدمات ممتازة في دعم هذا الجهاز وخاصة ان كانت هذه الخدمات مدفوعة وليست مجانية فان هذا النظام سيكون ممتاز وعلى الأقل فانك ستضمن مستوى معين من تقديم الخدمة لديك، كذلك يوجد نظام تكتيت نامير Ticket Number ليس كحال اغلب انظمة اللينكس حيث ان اخر ما لديهم هو منتدى خاص بالاعطال وخلافه وكل ما عليك فعله هو ترك مشاركة بالمنتدى لتحديث فيها عن العطل واعراضه وبعد العديد من محاولات الاصلاح فانه سيقول لك بكل بساطة ان ما لديك ما هو الا بوج BUG وانتظر التحديث القادم وان شاء الله ربنا سيوقفنا ونستطيع معرفة حل هذا الأمر وهكذا انت تكون مطالب اما انك ترجع اصداره للخلف لتلافي هذا العطل او انك تعايش العطل الى ان يكرمهم ربك بالحل من عنده، على الرغم ان سبب الدعم الفني غير هام بالنسبة الى سيسكو الا انها ميزة تجعل المستخدم لدى سيسكو مطمئن لهذا النظام خاصة في المراحل الأولى من التسويق.

**استهلاك الموارد Resources Consumption:** هذه النقطة يمكن يتشارك فيها كل انظمة اللينكس حيث ان المعروف ان اغلب سيرفرات لينكس بلا اية واجهات رسومية GUI الا اذا انت ركبت الواجهة التي تريد Gnome/KDE لكن هذه الجزئية او النقطة تستطيع توفير الكثير من استهلاك البروسيسور CPU والرام RAM وكذلك تجعل هذا الحل المبني على اللينكس بإمكانه ان يقوم بأكثر من عمليه Processes في نفس الوقت بلا اي ضغط على السيرفر، وكذلك مع تطور الهارد ويبيير أصبحنا نستطيع الكلام عن هذا الجزء العمليات تتزايد أكثر وأكثر.



# CALL PARK

بقلم: أحمد الشحات

## Call Park Configuration

### add new - call park - call routing من

The first screenshot shows the 'Call Park' configuration page in Cisco Unified CM Administration. The 'Call Park' tab is selected, and the 'Call Park' configuration is being set up. The 'Call Park' configuration is set to 'Call Park' and the 'Call Park' is set to 'Call Park'.

The second screenshot shows the 'Call Park Number Configuration' page. The 'Call Park Number/Range' is set to '12XX' and the 'Description' is set to 'my test call park'. The 'Partition' is set to '< None >' and the 'Cisco Unified Communications Manager' is set to '10.1.200.21'.

في هذه الصورة القادمة ترون أصبعي أولاً هذا هو الشيء المهم أما الشيء الثانوي فهو كلمة park الموجودة أعلى أصبعي



أخواني الاعزاء المبتدئين في عالم الفويس مقالنا اليوم سيختلف كثيرا عن المقالات السابقة التي تابناها سويا ففي السابق كنت اضع الدروس لمن لم يرى أي شيء من معدات الفويس ومن لم يخطوا خطوة واحدة في هذا الاتجاه أما اليوم فسننتقل سويا نقلة كبيرة جدا الى حيث عالم الاحتراف في الفويس .

فبعد تفكير عميق مع المهندس ايمون وجدت انه لن يسمح للمبتدئين بإنشاء الشبكة من الصفر بل سيعطونهم مهمة صيانة شبكة مؤسسة أو تشغيلها حتى يتم الاعتماد عليهم , فوضعت مقالتي الحالية وسلسلة المقالات القادمة التي تغطي الاحتراف في عالم استخدام والاستفادة من كل الامكانيات الموجودة في عالم الفويس

فليس من الطبيعي ان أقوم بتأسيس شبكة تكلفني مئات الآلاف من الجنيهات ثم لا استخدم منها الا خاصيتين فقط وهي الاتصال والاجابة على الاتصال فالامكانيات التي توجد في ip phone كثيرة جدا مما تجعل التليفون الواحد يعمل كأنه سنترال كامل وهذه الامكانيات هي سبب استخدام الشبكة أصلا

لنبدا على بركة الله

**سؤال :** ما المميزات الموجودة في هاتف سيسكو  
 pickup -pickup group -hunt group  
 ----park--conference - intercom -call pack-do not disturb  
 etc

وطبعا سنتناول كل خاصية بالتفصيل الممل

**الخاصية الاولى**

## Call park

هذه الخاصية ستمكن المستخدم من ركن المكالمات ؟  
 لا تستغربوا اللفظ هي فعلا خاصية لركن المكالمات في مكان ما واسترجاعها مرة أخرى مثل السيارة وركها في الموقف لحين الحاجة إليها ثم استرجاعها مرة أخرى

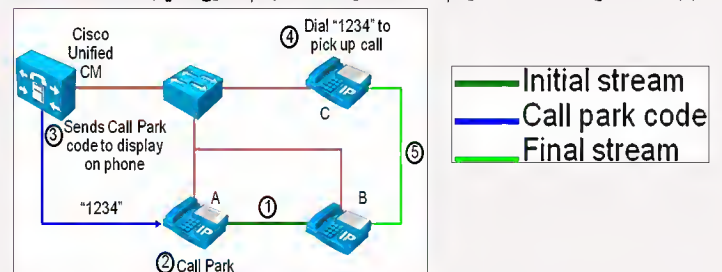
مثال  
 أنت مثلا على وشك الخروج من مكتبك والذهاب الى مكتب warior10 مثلا وفي لحظة قيامك من على المكتب اتصل بك شخص ولا تريد الجلوس مرة أخرى كل ما عليك فعله ستقوم برفع السماعة وعمل بارك للمكالمة وعندما تذهب لمكتب warior10 المجاور ليك ستقوم برفع السماعة وطلب رقم park ستأتي لك المكالمات مرة أخرى

الامر بسيط جدا بالنسبة لطريقة العمل  
 كل ما عليك فعله هو ضغط park بواسطة الضغط على park softkey الموجود في القائمة السفلية في التليفون وعند الضغط على هذا الزر سيظهر لك على الشاشة رقم ال park الذي تم تخزين المكالمات فيه لمدة عشر ثواني

**سؤال :** ما الذي سيحدث لو قام شخص اخر بعمل park لمكالمة أخرى  
 الإجابة : رقم ال park ليس رقم واحد بل هو مجموعة كبيرة من الأرقام أنت تحدد لها لحظة تأسيس الخاصية كما سنرى من المثال  
 فلو أنت عملت park في رقم 7000 مثلا فمن بعدك سيأخذ الرقم 7001 ومن بعده سيأخذ 7002 وهكذا

ملحوظة مهمة  
 خاصية call park تعمل على cucm منفردا بمعنى لو عندنا cluster يحتوي على أربع cucm فيجب أن يكون لكل cucm أرقام park مختلفة عن cucm الأخرى وذلك لأن CALLPARK يتم برمجتها على الكول مانيجر وليس على CLUSTER  
 ويمكن وضع رقم واحد أو مجموعة من الأرقام لتكون مخصصة لل PARK حتى 100 رقم بالنسبة للكول مانيجر الواحد ولا يمكن أن يحدث تداخل بين أرقام CALL PARK في السيرفرات المختلفة CUCM

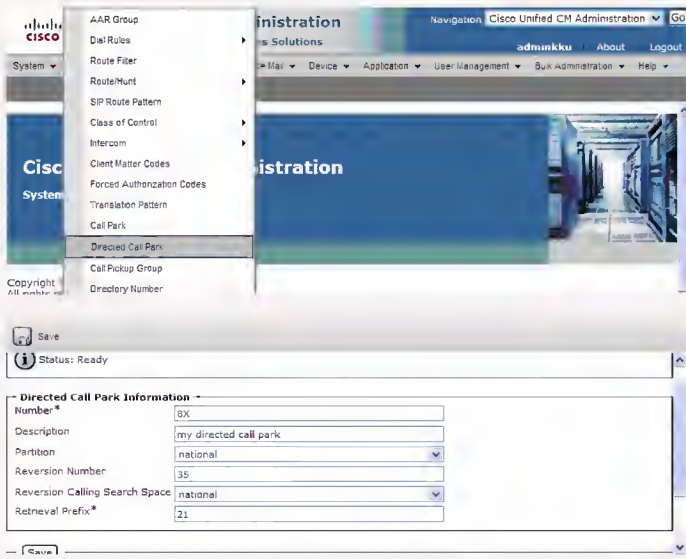
**سؤال :** كم عدد المكالمات التي يمكن عمل PARK لها في الرقم الواحد  
 الإجابة : مكالمات واحدة فقط لكل رقم المكالمات الأخرى تأخذ الرقم الفارغ الذي بعده



الشكل السابق يوضح عملية CALL PARK

- 1- المستخدم على التليفون A يقوم بالاتصال على التليفون B
- 2- المستخدم على التليفون A يريد أن يأخذ المكالمات الى غرفة الاجتماعات التي سيذهب اليها حالا (قام بالضغط على PARK SOFTKEY)
- 3- سيرفر CUCM الذي ينتمي اليه التليفون A سيرسل له أول رقم متاح من أرقام CALL PARK وسيكون هذا الرقم مثلا هو 1234 وسيظهر هذا الرقم على الشاشة للمستخدم A لمدة عشر ثواني لكي يحفظ الرقم
- 4- المستخدم الذي على تليفون A سيترك الغرفة ويذهب الى غرفة الاجتماعات حيث يوجد تليفون C سيرفع السماعة ويتصل بالرقم 1234 لكي يسترجع المكالمات المخزنة
- 5- النظام سيقوم بتأسيس المكالمات بين التليفون B وبين التليفون C





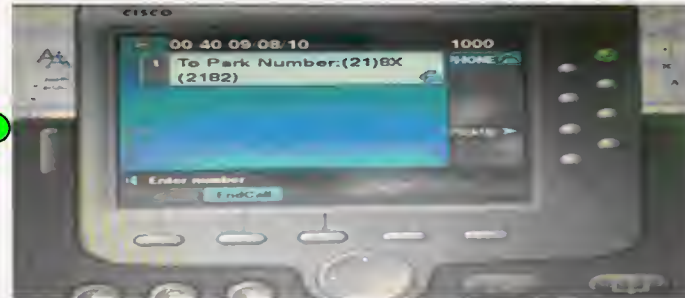
والآن سنرى بعض الصور من التليفونات حقيقية , في الصورة تلفيت الاتصال من التليفون رقم 1002



وفي هذه الصورة قمتم بعمل تحويل المكالمة على الرقم 28 وطبعاً التليفون فهم مباشرة أن هذه الرقم خاص بال Park فأضاف له x12 Prief المجددة بين قوسين وستكتمل عملية التحويل مباشرة بمجرد ضغط زر Transfer مرة أخرى كما سنرى في الصورة القادمة



في الصورة الأولى على اليسار قمتم بالضغط على زر transfer مرة أخرى ظهرت لنا الرسالة Call Park At 82 الموجودة بأفس الشاشة على اليسار أما الصورة الثانية فهي تفيد بأن المكالمة قد تم تحويله



والآن أنا ذهبت إلى تليفون آخر IP Communicator موجود عندي على الكمبيوتر وقمت بالاتصال بالرقم 2182 فظهرت لي الرسالة الموجودة بأعلى الشاشة أنه قد تم تحويله إلى Park رقم 218x وبأسفله رقم ال park 2182



وهكذا تم الاتصال بين التليفون رقم 2001 وبين التليفون رقم 0001 عن طريق تحويل المكالمة من التليفون رقم 1001

بعد الضغط على كلمة park ترون على الشاشة جملة call park at 7000 وهذا هو الرقم الذي وضعته من قبل لكي يكون مخصص ل call park وكما أخبرناكم سابقاً يمكن أن يكون رقم واحد مثل 7000 أو مجموعة من الأرقام مثل 12xx وهذا معناه من أول 1200 إلى 1299 لأن x احتمال من صفر إلى 9



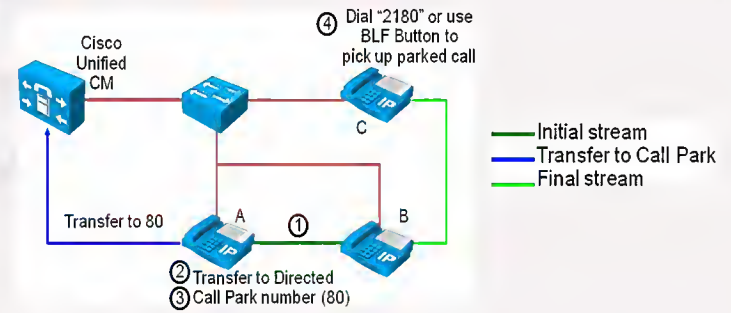
الآن قد انتهينا من النوع الأول من call park وهناك نوع آخر اسمه

الخاصية الثانية

## Directed call park

وهذا النوع مثل الأول تتم برمجته من call routing – directed call park التليفونات التي تدعم BLF (directed call park Busy Lamp Field) يمكن أن ترمج لكي تعرض حالات Idle /busy لأرقام directed call park التي يتم تحديدها المستخدم يستطيع أيضاً أن يستخدم BLF لكي يسرع الاتصال (زر الاتصال السريع) ب directed call park

**سؤال :** ما هي ميزة directed call park عن call park الاجابية : ي directed call park توجه المكالمة إلى الرقم الذي ستستخدمه أما call park فيتم تخصيص الرقم اتوماتيكياً لها بدون أي تدخل منها أو اختيار وبالمثل في هذه الحالة لا يمكن وضع أكثر من مكالمة واحدة في نفس directed call park ولاسترجاع المكالمة المخزنة فإن المستخدم يجب أن يتصل ب retrieval prefix متبوعاً برقم directed call park الذي تم تخزين المكالمة به وفي الشكل التالي طريقة عمل directed call park



- 1- المستخدم للتليفون A يتصل بالتليفون B ويؤسسوا اتصال بينهم
- 2- المستخدم للتليفون A يضغط soft key transfer ثم يتصل برقم directed call park ولكن الرقم 80
- 3- المستخدم A يضغط زر التحويل transfer مرة ثانية لكي تكتمل عملية التحويل ووضع المكالمة في directed call park رقم 80
- 4- المستخدم سيغادر إلى غرفة الاجتماعات حيث يوجد التليفون C ثم يرفع السماعة ويطلب الرقم 21 حيث أن هذا هو رقم Retrieval Prefix الذي قمنا بتعيينه أثناء عملية الترجمة كما سنرى لاحقاً ثم يطلب رقم 80 حيث أن هذا هو رقم directed park الذي تم تخزينه المكالمة به

5- بعد الاتصال بالرقم كامل وهو 2180 سيتم الاتصال بين التليفونين B و C

**سؤال :** ماذا سيحدث إذا لم يتم استقبال المكالمة خلال الوقت المحدد لها كأنني أثناء خرجي من مكتب قابلني موظف أضاع وقتي في أي حديث كالموظف إيهاب نصار مثلاً ولم يقم أحد غيري باستدعاء المكالمة من ال PARK

الاجابية : سيتم تحويل المكالمة إلى الرقم الذي قمنا بتعيينه في خانة Reversion Number DIRECTED CALL PARK هل هناك مواصفات معينة للتليفون الذي سيتم استخدامه لعمل

الاجابية : لا .

أي تليفون به خاصية TRANSFER يستطيع عمل DIRECTED CALL PARK وكما ذكرنا في CALL PARK العادي فإن DIRECTED CALL PARK يمكن أن يكون رقم واحد أو يكون مجموعة أرقام مثل 12XX فهذا يعني الأرقام من 1200 إلى 1299

## Directed Call Park Configuration CALL ROUTING -> Add New Directed Call Park



# طريقة إعداد الـ Static ARP

## على جونيير وسيسكو ولينوكس ومايكروسوفت

بقلم: أيمن النعيمي

```
C:\Windows\system32\cmd.exe

Interface: 192.168.0.2 --- 0xf
Internet Address      Physical Address      Type
192.168.0.1           00-0e-2e-9e-e2-be    dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
```

سوف أتطرق في هذه المقالة إلى موضوع هام وهو كيفية إعداد الـ Static Arp على كل من أجهزة سيسكو وجونيير بالإضافة إلى أنظمة لينوكس ومايكروسوفت ومما لاشك فيه أن هذا الموضوع على قدر كبير من الأهمية في رفع أداء الأجهزة على مستوى الروترات بالإضافة إلى الأمن والحماية على مستوى أنظمة التشغيل

### لماذا أقوم بإعداد Static Arp على أنظمة التشغيل ؟

هدفنا الأساسي من هذه العملية هي الامن والحماية فنحن نعلم أن هناك هجمات تقوم بتزوير الماك أدريس والتي تعرف بي الـ Arp spoofing والتي سوف أتحدث عنها قريباً إن شاء الله لذا سوف أقوم بربط الأيبي مع الماك أدريس الخاص فيه خوفاً من هذا النوع من الهجمات وطريقة الإعداد بسيطة جداً وهي موضحة بالصورة القادمة

```
C:\Windows\system32\cmd.exe

C:\Users\Ali>arp -s 192.168.10.1 00-13-ab-88-c6-09
```

كما هو واضح الأمر هو arp -s متبوعاً بي الأيبي والماك أدريس المطلوب وأخيراً إعداد الـ Static Arp على الأنظمة المفتوحة المصدر مثل لينوكس وأبنتوا والـ... فهي تتم من خلال الأمر التالي  
arp -i eth0 -s ip-address mac-address  
ولاننسى تحديد المنفذ أو كرت الشبكة المرتبط مع الروتر أو مع أحد الأجهزة الموجودة على الشبكة والذي يعبر عنه بي eth0

### لماذا أقوم بإعداد Static Arp على الروترات ؟

لكي أجيبك على السؤال يحتاج الأمر مني أن أعود قليلاً لبعض الأساسات التي درسناها في الشبكات فكمنا نعلم أن البايكيت التي تصل إلى الروتر يتم عمل Deencapsulate للبايكيت ويتم إعادة تغيير الماك أدريس الـ Source Arp الـ Destination لكي تطابق الـ Next Hop وغالباً ما يعود الروتر إلى الـ Table أو Arp cashe لمعرفة هذه التفاصيل فإن لم يجد مطلبه فسوف يتم إرسال Arp Request للوصول إلى الماك أدريس المطلوب وطبعاً عملية اختيار الـ Next Hop IP يتم الوصول إليها من خلال الـ Routing Table وهي الفكرة التي أردت توصيلها لك فعوضاً عن قيام الروتر بهذه العملية سوف نقوم بربط الأيبي بالماك أدريس الخاص فيه بشكل يدوي وذلك من خلال الـ Static ARP بهدف رفع أداء الروتر ولو كان هذا الرفع شيء بسيط لكن مفيد في نفس الوقت ولكي نقوم بالإعداد على أجهزة سيسكو نقوم بكتابة الأمر التالي في الـ Configuration Mode

```
IOS

arp ip-address hardware-address type [alias]
```

كما هو واضح من الأمر نقوم بكتابة الأمر arp وبعدها نقوم بكتابة الأيبي والماك أدريس الخاص فيه وكلمة Type من أجل Encapsulation description فقط فلو كان المنفذ من نوع إيثرنت فهي سوف تكون arpa أما لو كان المنفذ فايبر فهي سوف تكون Snap أما بالإضافة الأخيرة Alies فهي اختيارية لتمكين الـ IOS من الرد على طلبات الـ Arp Request على أساس أن هذا الأيبي هو خاص فيه .

أما طريقة الإعداد على أجهزة جونيير فهي تتم أولاً بالتوجه إلى المسار التالي  
[edit interfaces interface-name unit logical-unit-number family inet address address]

ونقوم بكتابة الأمر التالي :

```
Set arp ip-address (mac) mac-address
```

بحيث نضع مكان ip address الأيبي المطلوب ونفس الشيء مع خانة الـ mac-address

## كيفية حفظ وأسترجاع نسخة من الإعدادات على أجهزة جونيير

أما كيفية أسترجاع الإعدادات عند الحاجة سوف نتوجه أولا إلى المكان التالي  
 root@switch# edit system archival configuration  
 نقوم أولا بكتابة الأمر التالي load merge وبعدها نكتب أسم المستخدم وكلمة السر وأيبي السيرفر وبعدها أسم الملف الخاص بالإعدادات التي تريد أسترجاعها وهي مبنية بالإعدادات التالية

```
Junos's juniper
edit system archival configuration]]
root@switch# load merge ftp://username:password@192.168.1.1
/switch_juniper.conf.gz
load complete
edit system archival configuration]]
#root@switch
```

أما بالنسبة للروتات فافضل طريقة من أجل حفظ الإعدادات هي من خلال ال J-web الذي تحدثنا عن طريقة تشغيله في الأعداد السابقة هذا مالمدي لمتابعي جونيير وأن شاء الله سوف نتوسع أكثر في جونيير في المستقبل القريب

سوف نتحدث في هذه المقالة والتي أخصصها لكل محبي ومتابعي أجهزة جونيير عن كيفية عمل نسخة احتياطية من الإعدادات أو ال Configuration File بشكل أوتوماتيكي وأقصد بشكل أوتوماتيكي أي كل مرة يتم كتابة الأمر Commit في موجه الأوامر وطبعاً كيفية أسترجاع الإعدادات عند الحاجة التطبيق سوف يكون على سويتشات جونيير المعروفة بي EX Series وعلى سيرفر FTP وهذه هي الإعدادات الخاصة بعمل نسخة احتياطية عند تطبيق الأمر Commit والتي سوف تلاحظه عند كلمة transfer-on commit

```
Junos's Juniper
system {
  archival {
    configuration {
      transfer-on-commit;
      archive-sites {
        ;"ftp://username:password@192.168.1.1"
      }
    }
  }
}
```

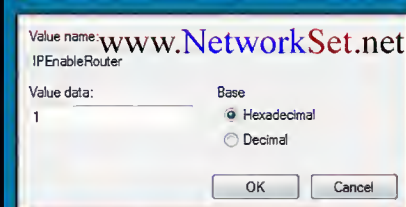
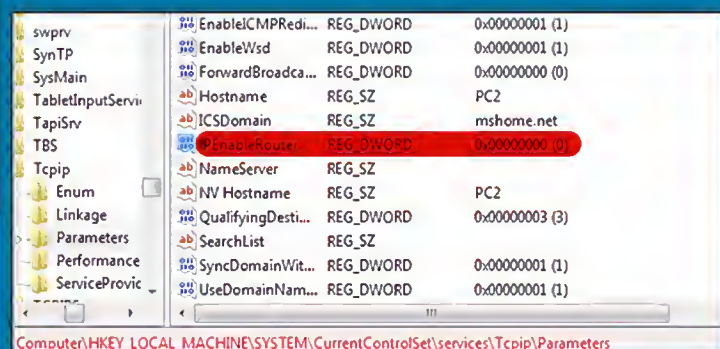
ولاتنسى تغيير ال Username وكلمة السر إلى الإعدادات الخاصة بسيرفر ال FTP الذي لديك وأخيراً نضع أيبي السيرفر

## كيف تقوم بتحويل ويندوز أكس بي إلى روتر!

فسوف نقوم بكتابة الأيبي بناء على إعدادات الروتر ولنفرض أنها على الشكل الآتي  
 IP=192.168.3.2, Mask=255.255.255.0, Gateway=192.168.3.1  
 ولندخل الآن في الجد نتوجه إلى Start->Run->regedit ونتجه إلى المكان التالي

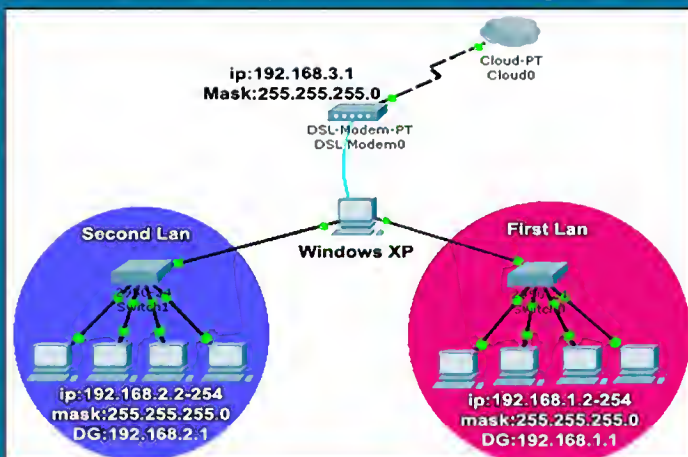
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters

ونبحث عن القيمة التالية IPEnableRouter ونضغط عليه مرتان ونقوم بتغيير الرقم من صفر إلى واحد كما في الشكل القادم



وأخيراً نقوم بعمل إعادة أطلاق للويندوز وهي خطوة مهمة لكي تنجح الطريقة ومبروك عليك الروتر البسيط تم تجربة هذه الطريقة أيضاً على ويندوز سيرفر

مقالة حصريّة ومفيدة جداً لمتابعي مجلتنا العزيزة وهي كيفية تحويل ويندوز أكس بي إلى روتر لكن بطريقة بسيطة ويهدف ربط ثلاث أو أربع شبكات مع الإنترنت بالإضافة إلى إمكانية ربط هذه الشبكات مع بعضها البعض وبالتالي توفر على نفسك شراء روتر مخصص لهذه العملية قبل أن نبدا الشرح سوف نأخذ هذه الصورة ونقوم بالتطبيق عليها



وكما يتضح من الصورة نجد أمامنا شبكتان متصلتان مع ويندوز أكس بي والذي بدوره يتصل مع الإنترنت لذا تحتاج هذه العملية إلى وجود ثلاث كروت شبكة (ICN) الأول متصل مع الشبكة رقم واحد ويملك الإعدادات التالية فقط IP=192.168.1.1, Mask=255.255.255.0 ونفس الشيء مع الكرت الثاني مع تغيير عنوان الشبكة IP=192.168.2.1, Mask=255.255.255.0 وأرجو أن تلاحظ أنني لم أكتب أي شيء في خانة ال Gateway أما الكرت المتصل مع الإنترنت والذي يكون مودم DSL



قد يكون أسهل طريق لتحويل الأيبي 4 إلى الأيبي 6 يتم من خلال تحويل الأول إلى الـ Binary وبعدها نقوم بتحويله إلى الـ HEX وطبعا العملية طويلة وتأخذ الكثير من الوقت لذا تدوينتي لهذا اليوم سوف تكون عبارة عن طريقة سريعة وبسيطة لتحويل الأيبي من IPv4 إلى IPv6 وبالعكس

# Converting

## IPv4 ↔ IPv6

بقلم: أيمن النعيمي

القسم الرابع 91 / 16 = 5 وباقي القسمة سوف تكون 11 والنتيجة النهائية سوف تكون 5B  
نتيجة كل ماسبق سوف يكون الأيبي 192.168.120.91 بالهيكس تساوي COA8:785B وبالتالي سوف يكون شكل الـ IPv6 كالآتي:

2002:COA8:785B::1/64

قبل أن أبدا سوف تسألني ما حاجتي لتعلم هذه الطريقة ؟ نحتاج هذه الطريقة عند استخدامنا للـ IPv6 tunnels وخاصة الـ 6to4 نقوم عادة باستخدام أيبي مخصص وهو 16 / : : 2002 والذي من خلاله نقوم بكتابة الأيبي 4 لكن بالهيكس وبكلام آخر نقوم بإضافة الأيبي وفق الشكل التالي

2002:(IPv4 address in Hex):(16 bit network number in Hex)::/64

أما للقيام بعكس العملية أي تحويل الـ IPv6 إلى IPv4 فسوف نقوم بالتطبيق على المثال نفسه وأول خطوة سوف قوم بها هي كتابة الأرقام الموجودة على شكل ثنائي أي بالشكل التالي C0 A8 78 5B ونأخذ كل قسم منها على حدى C0 أول خطوة سوف نقوم بتحويل أرقام الـ HEX إلى Decimal وفق المعادلة التالية

$$((C=12) * 16) + (0 * 1) = 192$$

A8 سوف تحسب بنفس الطريقة الثابتة أي بالشكل التالي

$$((A=10) * 16) + (8 * 1) = 168$$

$$78 = 120 + (7 * 16) + (8 * 1) \text{ تساوي } 78$$

$$5B = 91 + (5 * 16) + (11 * 1) \text{ تساوي } 5B$$

وكما تشاهدون أن الخانة الثانية مخصصة لكتابة الأيبي لكن في الـ HEX لذا يتوجب علينا القيام بهذه العملية بأنفسنا وللتحويل سوف نتبع هذه الطريقة السريعة ولنأخذ هذا المثال الصغير 192.168.120.91  
لنأخذ كل قسم على حدى

القسم الأول 192 نقوم بتقسيمه على 16 وسوف تكون النتيجة 12 والباقي صفر والـ 12 بلغة الهيكس تساوي C ونكتب بعدها باقي القسمة لتكون النتيجة C0

القسم الثاني 168 نقوم أيضا بنفس العملية أي تقسيمه على 16 وتكون النتيجة 10 وباقي القسمة 8 والـ 10 بلغة الهيكس تساوي A والنتيجة النهائية سوف تكون A8

القسم الثالث 120 / 16 = 7 وباقي القسمة سوف يكون 8 والنتيجة النهائية سوف تكون 78

## ما هو الـ Passive Interface

### وما فائدة إستخدامه ؟

بقلم: أيمن النعيمي

والسؤال الذي سوف أوجه إليك لماذا لا أقوم بإضافة الوايلد ماسك للشبكة في إعدادات الـ EIGRP وأنتهي من هذه المشكلة بدون أمر الـ Passive Interface ؟؟؟  
OSPF

بالنسبة لهذا البروتوكول فالموضوع هو ذاته في الـ EIGRP يعني يمنع إرسال أي Routing Information ويمنع أيضا إرسال Adjacency بين الروترات والتي تعد مسؤولة عن عملية relationship between two OSPF routers  
RIP

بالنسبة للـ RIP فالعملية تختلف قليلا لأن الـ Passive Interface هنا سوف يمنع إرسال أي معلومات من خلال إيقاف الملتى كاست أيبي المسؤول عن عملية الإرسال لكن سوف يقوم بالاستماع للتجديقات التي سوف تصله من خلال هذا المنفذ ومن روترات أخرى الشيء الأخير الذي أحب أن أضيفه وهو يتعلق بموضوع إعداد الـ Passive Interface لاننا نستطيع أن ندخل على الـ Routing Mode وكتابة الأمر Passive interface default والذي سوف يقوم بوضع كل المنافذ الموجودة في حالة Passive وبعدها أقوم بكتابة الأمر no passive-interface fastethernet 0/0 لكي أقوم بتفعيل المنفذ 0/0 لكي يتم إرسال المعلومات إليه يعني ببساطة قمت بعكس العملية السابقة ففوضا عن تحديد من هو الـ Passive وضعت الجميع في حالة الـ Passive وبعدها قمت بتحديد من هو الذي يجب أن يعمل أتمنى أن تكون هذه التدوينة قد أجابة على السؤال وأفادت الجميع ودمتم بود

## EIGRP

يستخدم أمر الـ Passive Interface في هذا البروتوكول لمنع إعلان بعض الشبكات الموجودة على الروتر من إرسالها إلى روترات أخرى وبكلام آخر نستخدم هذا الأمر لمنع البروتوكول من إرسال الـ Routing information لأحد الشبكات المتصلة معه إلى بعض المنافذ التي نقوم نحن بتحديددها بينما يسمح لباقي المنافذ بإرسال المعلومات النقطة الثانية وهي الأهم وهي تطبيق هذا الأمر على بروتوكول الـ EIGRP سوف لن يسمح فقط بإرسال الـ Advertisement بل وسوف يمنع إقامة أي علاقة بين الروترات المتصلة مع هذا المنفذ وبمعنى آخر سوف يمنع إقامة أي Relationship With the neighbors والسبب لأن هذه الخاصية سوف تمنع الروتر من إرسال الـ hello Msg والتي سوف تنعكس على إرسال واستلام الـ Routing Update بين الروترات أما الفائدة من هذا الموضوع فسوف تتوضح من خلال هذا المثال إن شاء الله

```
Cisco's IOS
Router(config)#interface fastethernet 0/0
Router(config-if)# ip address 192.168.0.1 255.255.255.0
Router(config)#interface fastethernet 0/1
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Router(config)#router eigrp 10
Router(config-router)#network 192.168.0.0
Router(config-router)#passive interface fastethernet 0/1
```

لو أستثنينا آخر أمر في هذا المثال سوف يقوم الـ EIGRP بالأعلان والتواصل مع المنافذ 0/0 و 0/1 ونحن في حقيقة الأمر لانريد للشبكة الثانية أن يتم إرسال إليها أي شيء يخص الـ Routing Informations لذا أقوم بكتابة الأمر Passive interface بالنسبة للمنفذ 0/1 وبهذا أ منع إرسال أي كل هذه الأشياء تنعكس على موضوع الأمن والسيكورتى فقد اكون هذه الشبكة متصلة مع شركة أخرى أو أي شيء آخر ونحن لانريد للـ Routing Informations أن يتم إرساله إلى هذه النقطة وأخيرا نوفر بعض الشيء من الـ CPU على الروتر .





# قسم أمن وحماية الشبكات

هذا القسم سوف يتم عرض فيه كل الأمور الواجب عملها في الشبكة بهدف التخفيف من نسبة القرصنة التي تحدث على الشبكة وأرجو منك أن تدقق على كلمة تخفيف لان النظرية العامة تقول لا يوجد جهاز آمن خالي من الثغرات مهم كانت قوته!

## الطريق الى السيورتي

بقلم: محمود عمر

بعد ان تكلمنا عن انواع الهاكرز و التعريف بهم في العدد السابق للمجلة نحتاج الى التكلم عن بعض المصطلحات الهامة في عالم السيورتي و من الهام ان تكون على فهم و دراية بها . بعدها سوف نتطرق إلى موضوع آخر نتكلم عن الأسباب التي تدفعنا إلى الاهتمام بعالم الأمن والحماية



"سوف نقوم في الاعداد اللاحقة بعمل مقارنة بين الويندوز و الليونكس من الجانب الامنى"

### مشكلة في التصميم : Design

وهي ليست مشكلة في الانظمة ولكنها مشكلة في التصميم مثل المشكلة في تصميم ال TCP/IP وخصوصا المشكلة الشهيرة التي كانت محور كلام محترفين السيورتي منذ اواخر عام 2008 حتى الان و هي مشكلة في تصميم ال DNS فا كما نعرف ان هناك DNS Server 13 او كما يسمو ال Root Hint DNS Servers و اماكنهم موزعة على مستوى العالم لمزيد من التفاصيل عن ال Root Name Server

<http://en.wikipedia.org/wiki/Root.servers> و قد كانت المشكلة في ال DNS و ثغرة ال DNS cache poisoning مما لزم لى التحديث الى بروتوكول جديد لل DNS و يسمى بى ال DNS Security (DNS SEC) Hashed Authenticated Denial of Existence

و هو المستخدم فى IPV6 ايضا ولمزيد من التفاصيل عنة اتبع الرابط التالى و ان شاء الله سوف نتكلم عنة بالتفصيل لاحقا <http://tools.ietf.org/html/rfc5155>

### اخيرا خطا في الاعدادات Configuration للنظام و البرمجيات :

هذه المشكلة تكون من المستخدم نفسة وليس من النظام فا تكمن المشكلة فى خطا فى الاعدادات مثل ترك Open Port لا داعى منها والتي تمكن الهاكر من اختراق جهازك مثل SMB over TCP file Sharing Port 445 او خطا فى اعداد الفايروال Firewall مثل ترك منافذ مفتوحة و خدمات تعمل دون الحاجة لها تمكن من خلالها استغلال هذه الثغرة و الدخول منها والتي يمكن تفاديها بتفيذ اعدادات صحيحة

### Vulnerability (ثغرة) :

نقطة ضعف (Weakness Point) فى النظام System او فى مشكلة فى التصميم Design او خطا فى الاعدادات Configuration للنظام و نقاط الضعف هذه التي يستطيع ان يتسلل منها الهاكر و يقوم باختراق و احدث دمار فى البيانات والانظمة .

لنأخذ مثال لكي تتضح الأمور بشكل أفضل

نقطة ضعف فى النظام System : وهو تتمثل فى مشاكل او اخطاء برمجية فى النظام يكتشفها المخترق و من خلالها يتم اختراق الجهاز و التسلل منها وأفضل مثال على هذا النوع من الثغرات هي الثغرات التي تظهر فى الانترنت اكسبلورر Internet Explorer او الثغرة التي اكتشفت فى ويندوز سيفن Windows 7 وايضا ويندوز Server 2008

منذ تقريبا شهر من الان وكانت من نوع "buffer overflow error" والتي تمكن المهاجم الذي يمتلك صلاحيات مستخدم على النظام من تنفيذ هجوم يؤدي لحجب الخدمة (ظهور الشاشة الزرقاء) مع وجود احتمال لتخطي الصلاحيات المحددة له في حال استغلال الثغرة بشكل صحيح (Privilege Escalation) . وفى اغلب الاحيان يتم علاج مثل هذا النوع من المشاكل أو الثغرات التي تستهدف النظام هو تنزيل ال Hot Fixes والتي دائما ميكروسوفت بتوفيره لعلاج المشكلة لذلك من الهام جدا دائما تنزل ال التحديثات لكل المنتجات لتفادي حدوث مثل هذه الاختراقات

ولكن المشكلة تكمن فى وقت ظهور الثغرة ووقت صدور التحديث من الشركة !!!!!!! وطبعاً نقاط الضعف لا توجد فقط فى انظمة ميكروسوفت فقط فقد كان هذا فقط مثالا للتوضيح فمنها من هو موجود فى الليونكس و انظمة ماك و ايضا البرامج المثبتة على الانظمة و الخدمات الموجودة مثل سيرفر ال IIS فى حالة الوندوز او ال Apache فى حالة الليونكس و لنا كلام عنهما كثيرا لكثرة ثغرتهم و من اشهر المواقع لقراءة الثغرات و التعرف على الجديد منها

<http://nvd.nist.gov/>

<http://www.securityfocus.com/vulnerabilities>



## التهديد (Threat) :

وهو امكانية استغلال الثغرات التي تمكن ال Attacker من الدخول الى نظامك وسرقة او تخريب البيانات مستخدم ال Exploit

## Exploit : استغلال او استثمار الثغرات

وهي اكود مكتوبة بلغات برمجية تستطيع بها استغلال الثغرات واختراق الاجهزة والسيرفرات بها وهناك مواقع تكتب طريقة استغلال الثغرات الجديدة والتي عادة يطلق عليها Zero Day Exploit فبمجرد ظهور ثغرة سريعا ما يقوم المبرمجون بكتابة اكود او ال Exploit لطريقة استغلال هذه الثغرة وكيفية الاختراق عن طريقها .

حان الان الوقت لنتكلم عن لماذا نهتم بالسيكورتى وما هي عوامل السيكورتى بعد ان فهمنا بعض المصطلحات الهامة في عالم السيكورتى فهناك اربع نقاط يجب ان تكون متوافرة في تصميمك في عالم السيكورتى لا غنى عنهم

سرية المعلومات Confidentiality

سلامة المعلومات Data Integrity

التأكد من انك الشخص المصرح له بالدخول على البيانات والمعلومات Authenticity

ضمان الوصول الى المعلومات والبيانات في اى وقت . Availability

## Confidentiality سرية المعلومات :

وهي عملية تشفير البيانات وحمايتها من السرقة مثل استخدام IP Sec او استخدام ال Certificates لتشفير البيانات عند نقلها من حاسوب الى اخر فلو فرضنا ان هناك متسلسل استطاع ان يراقب الترافك واستطاع ان يستخدم احد برامج التحليل Wire shark التي تحلل الترافك وتحويلها الى بيانات يمكن قرائته فعند تشفير البيانات لن يستطيع المتسلسل ان يفهم ما هذه البيانات وسوف تكون دون اى فائدة وبذلك نكون قد حققنا اول شرط من عوامل الامان

## Data Integrity سلامة البيانات:

وهي المحافظة على البيانات دون الوصول اليها وحمايتها من التغير والتلاعب بها دون الحصول على اذن او تصريح بعمل ذلك ولنضرب مثالا لتخيل ان لك صديق في اى شركات المحمول يعمل في مجال ال IT كيف تضمن الشركة ان هذا الشخص لن يقوم بالتلاعب في بيانات الفواتير الخاصة بالعملاء او مثلا لو عندك في الشركة هناك نظام حضور وانصراف مبني على Finger Print وقاعدة بيانات من يضمن ان لن يتلاعب احدا في قاعدة البيانات والتغير فيها لمصلحة احد الموظفين او مثلا تغير ارقام في بعض التحويلات من 10 الى 1000 على سبيل المثال

كل هذه الأمثلة تندرج تحت ما يسمى بى سلامة البيانات او Data Integrity او مثلا تريد ان تحمل احد البرامج من الانترنت من يضمن انه لم يتلاعب به احد المتطفلين ومثلان زرع Trojan في البرنامج لذلك احيانا عند تنزيل برامج ترى ما يسمى بال ال Hash وهو رقم يعتبر بمثابة البصمة لهذا البرنامج فلو قمت بتنزيل البرنامج ووجدت ان هذا الرقم او ال Hash مختلف فانهذا معناه ان هناك من تلاعب في هذا البرنامج وقام بعمل تغيير فيه .

## Authenticity التأكد من هوية الشخص و انك المصرح له بالدخول على البيانات والمعلومات :

وهي التأكد من الشخص المراد والمصرح له بالدخول على هذه المعلومات مثل لو كان لدينا Active Directory وهو المسؤول عن اعطاء الطلاحيات للمستخدمين في الشركة وقام مدير الشبكة باعطاء مستخدم صلاحيات لى قراءة ملف معين والتأكد انه ليس لديه الصلاحيات من التعديل عليها فهذه ما يسمى بعملية ال Authentication

## Availability ضمان الوصول الى المعلومات والبيانات في اى وقت واتاحتها دائما :

من العناصر الهامة جدا بعد التأكد من سلامة البيانات وتشفيرها والتأكد من

صلاحيات المستخدم وان تكون البيانات متاحة ونستطيع الدخول عليها اى وقت دون مشاكل فا اذا طبقنا كل ما سبق دون الحرص على امكانية الوصول الى البيانات فما الفائدة وهناك تدابير كثيرة للتأكد من الحصول على البيانات في اى وقت ومثال لذلك

ماذا يحدث اذا حدث عطل في النظام او احد السرفرات التي تحمل البيانات فبذلك نكون قد فقدنا كل البيانات ولذلك يمكن عمل ما يسمى بال Clustering و هي ايجاد سيرفر اخر مطابق تماما للسيرفر الاول في حالة عطل احدهما يعمل الاخر تلقائيا دون وجود Down Time ومن اشهر الهجمات على هذه النقطة هي هجمات حجب الخدمة Denial of Service Attack

ناتى الان الى اهم نقطة في حلقة اليوم وهي كيفية تصميم السيكورتى وما هي العوامل التي تؤثر و كيفية الاختيار بين اهم ثلاث نقاط وهم

1- Functionality

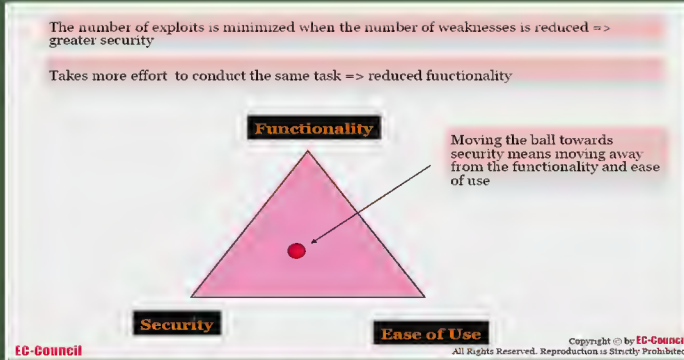
2- Security

3- Ease Of Use

عند تصميم الشبكة والسيكورتى الخاص بها دائما هناك نقطة خلاف كبيرة جدا وتعارض بين ال Security و ال Performance فمن المعروف ان بينهم علاقة عكسية فعند الاهتمام بالسيكورتى يقل اداء التتورك ومثال على ذلك نقل بيانات مشفرة تأخذ وقت اكثر من نقل بيانات غير مشفرة لانها تأخذ وقت في عملية التشفير وفك التشفير والذي ينعكس على الاداء بشكل عام ايضا يختلف اداء التتورك من وجود فايروال واحد او وجود اكثر من فايروال لذلك يصعب الاختيار ما بين السيكورتى وسرعة الاداء والشكل التالي يشرح هذه المشكلة وكيفية عمل التصميم المناسب لك .

قبل الشرح حاول ان تفكر معي اين يجب وضع هذه النقطة في المثلث هل بالقرب من

Functionality او ال Security او ال Ease Of Use ولماذا يجب الاهتمام ب ال Security و ال Functionality على سبيل المثال



الان ماذا كانت اجابتك هل تحريك النقطة بالقرب من ايهم ولماذا ؟ ام فكرت ان تضعها في المنتصف !!! هل تعلم ان جميع الاجابات صحيحة !!!!!!!

اذا ماذا يجب ان نختار وكيف وعلى اي اساس نختار ؟ هذه هي المشكلة التي تحير الكثير عند التصميم ولكن الموضوع بسيط ولا يحتاج الى الكثير من الجهد فالاحل الانسب هو مختلف دائما من مكان الى اخر على حسب الاتي : نوع البيانات واهميتها وايهما اهم بين السيكورتى او الاداء مثال للتوضيح حاول ان تفكر معي هل البنك يهتم اكثر بالسيكورتى ام سرعة الاداء وطبعا وبدون تفكير البيانات الموجودة في البنك تكون حساسة جدا وهامة للغاية لذلك يتم زيادة السيكورتى الى ابعد الحدود واذكر في احد البنوك قمنا بعمل تصميم 7 Different Layer of Security ولكن في شركة صغيرة لا تهتم بالسيكورتى لدرجة كبيرة ولكن تحتاج سرعة في نقل البيانات لذلك تذهب الكورة والاختيار الى ال Functionality

نستنتج من ذلك انه لا يوجد حل امثل فا التصميم يكون Case by Case تكلمنا كثير هذه الحلقة عن تعريفات وتعلمنا اهمية وعوامل السيكورتى الاساسية بذلك نكون انتهينا من ثانی حلقات الطريق الى السيكورتى. انتظرونى الحلقة القادمة أن شاء الله.



# عتاك و معلومات

أعداد عثمان إسماعيل

## CISCO SYSTEMS



RAM	128 MB(installed)/384 MB(MAX)-SDRAM
Flash memory	32 MB(installed)/128 MB (MAX)
Type	DSL modem
MAX Transfer Rate	24 MBps
Encryption Algorithm	DES , Triple DES , AES
Supplied OS	CISCO IOS
Digital Signaling Protocol	ADSL , ADSL2 , ADSL2+
DCP	Ethernet , Fast Ethernet
Protocol Remot	SNMP
Interfaces	2 x network -Ethernet 10Base - T/100Base -TX - RJ-45 1 x management - console - RJ - 45 Serial - auxiliary - RJ-45 1 x modem ADSL
MAX Temp 40 C , MIN Temp 0 C , VPN Support , support IP Sec ,	



**Router1841-ADSL**

RAM	64 MB
Flash memory	32 MB
Ramer Table of MAC Addr	8 K entries
Authentication method	RADIUS , TACACS+ , Secure SHELL v.2
Interfaces	48 x network - Ethernet - RG 45
Connection Type	Hulf-duplex , Full-duplex
Data Rate	1 Gbps
DCP	Ethernet , Fast Ethernet , Gigabit Ethernet
Protocol Remote	SNMP1 , RMON , Telnet , SNMP3 , SNMP2c
Number of Ports	48 x Ethernet 10Base -T , Ethernet 100Base - TX , Ethernet 1000Base -T
MAX TEmP 40 c , MIN Temp 0 c , DHCP Support , VLAN Support , IGMP snooping , auto MDI/MDI-X , DHCP snooping	



**SWITCH WS-C2960G**

RAM	128 MB (installed) / 483 MB (max)
Flash memory	64 MB (installed) / 128 MB (max)
Protocol Remote	SNMP 3
Type	DSU/CSU
Interfaces	2 x network - Ethernet 10Base-T/ 100Base-TX - RJ-45 1 x USB 1 x network - auxiliary 1 x management - console
Encryption	DES, Triple DES, AES
Supplied OS	Cisco IOS
OS Required	Microsoft Windows 98 Second Edition
DCP	Ethernet, Fast Ethernet
MPLS support , min temp 0 °C , max temp 40 °C, Humidity 10 - 85%	



**Router 2801**





# Juniper®

## NETWORKS

Maximum Performance and Capacity	Network Connectivity	Routing, Virtualization, Encapsulations
<ul style="list-style-type: none"> <li>* Junos Software Version Support: Junos Software 9.1</li> <li>* Firewall Performance (Large Packets): 750 Mbps</li> <li>* Firewall Performance (IMIX): 500 Mbps</li> <li>* Firewall and Routing PPS (64 Byte): 200,000 pps</li> <li>* 3DES and SHA-1 VPN Performance: 160 Mbps</li> <li>* Concurrent VPN Tunnels: 512 MB / 1 GB DRAM 256 / 512</li> <li>* Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 64 K / 128 K</li> <li>* New Sessions/Second: 5,000</li> <li>* Maximum Security Policies: 2048 (1 GB DRAM)</li> </ul>	<ul style="list-style-type: none"> <li>* Fixed I/O: 4 x 10/100/1000</li> <li>* Maximum PIM Slots: 5</li> <li>* Maximum EPIM Slots: 0</li> </ul>	<ul style="list-style-type: none"> <li>* BGP, OSPF, RIP, Static, ECMP: Yes</li> <li>* Multicast, PIM SM, SSM, IGMP: Yes</li> <li>* Maximum Number of Security Zones: 50</li> <li>* Maximum Number of VLANs: 256</li> <li>* PPP, FR, MLPP, MLFR, HDLC: Yes</li> </ul>

### Router J2350



Maximum Performance and Capacity	Network Connectivity	Routing, Virtualization, Encapsulations
<ul style="list-style-type: none"> <li>* ScreenOS version tested: ScreenOS 6.2</li> <li>* Firewall Perf (Large Packets): 1+ Gbps</li> <li>* Firewall Performance (IMIX): 1 Gbps</li> <li>* Firewall Packets Per Second: 600,000 PPS</li> <li>* 3DES+SHA-1 VPN Perf: 600 Mbps</li> <li>* Concurrent VPN Tunnels: 1,000</li> </ul>	<ul style="list-style-type: none"> <li>* Max Concurrent Sessions: 256,000</li> <li>* New Sessions/Second: 15,000</li> <li>* Max Security Policies: 4,000</li> <li>* Max Security Zones: 60</li> <li>* Max Virtual Routers: 16</li> <li>* Max Virtual LANs: 150</li> </ul>	<ul style="list-style-type: none"> <li>* Fixed I/O: 4x10/100/1000</li> <li>* Mini-Physical Interface Module Expansion Slots: 0</li> <li>* Physical Interface Module Expansion Slots: 2</li> <li>* Enhanced PIM (EPIM) Expansion Slots: 4</li> </ul>


### Switch SSG-550M



Maximum Performance and Capacity	Network Connectivity	Routing, Virtualization, Encapsulations
<ul style="list-style-type: none"> <li>* Junos Software Version Support: Junos Software 9.1</li> <li>* Firewall Performance (Large Packets): 600 Mbps</li> <li>* Firewall Performance (IMIX): 400M</li> <li>* Firewall and Routing PPS (64 Byte): 175,000 pps</li> <li>* 3DES and SHA-1 VPN Performance: 140 Mbps</li> <li>* Concurrent VPN Tunnels: 512 MB / 1 GB DRAM 256 / 512</li> <li>* Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 64 K / 128 K</li> <li>* New Sessions/Second: 5,000</li> </ul>	<ul style="list-style-type: none"> <li>* Fixed I/O: 4 x 10/100/1000</li> <li>* Maximum PIM Slots: 3</li> <li>* Maximum EPIM Slots: 0</li> </ul>	<ul style="list-style-type: none"> <li>* BGP, OSPF, RIP, Static, ECMP: Yes</li> <li>* Multicast, PIM SM, SSM, IGMP: Yes</li> <li>* Maximum Number of Security Zones: 40</li> <li>* Maximum Number of Virtual Routers: Yes</li> <li>* Maximum Number of VLANs: 256</li> <li>* PPP, FR, MLPP, MLFR, HDLC: Yes</li> </ul>

### Router J2320



Data Rate	Resiliency	MAC Addresses
<ul style="list-style-type: none"> <li>* 480 Gbps</li> </ul>	<ul style="list-style-type: none"> <li>Dual load-sharing internal autosensing AC power supplies</li> </ul>	<ul style="list-style-type: none"> <li>16,000</li> </ul>
Throughput	Power Options	Jumbo Frames
<ul style="list-style-type: none"> <li>* 357 Mpps (wire speed)</li> </ul>	<ul style="list-style-type: none"> <li>Autosensing; 110/220 VAC; 60/50 Hz</li> </ul>	<ul style="list-style-type: none"> <li>9216 Bytes</li> </ul>
10/100/1000BASE-T Port Densities	Operating System	IPv4 Unicast / Multicast Routes
<ul style="list-style-type: none"> <li>24 (dual-mode 1/10GbE network ports)</li> </ul>	<ul style="list-style-type: none"> <li>JUNOS</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>
10GBASE-X Port Densities	QoS Queues / Port	Number of VLANs
<ul style="list-style-type: none"> <li>24</li> </ul>	<ul style="list-style-type: none"> <li>8</li> </ul>	<ul style="list-style-type: none"> <li>1,024</li> </ul>
100BASE-FX / 1000BASE-X (SFP) Port Densities	Traffic Monitoring	Switch EX2500
<ul style="list-style-type: none"> <li>N/A</li> </ul>	<ul style="list-style-type: none"> <li>N/A</li> </ul>	

# مصطلحات تقنية

إعداد: أيمن النعيمي

**REPEATERS** : وهو أحد الأجهزة الخاصة بالشبكات ووظيفته الأساسية هي تقوية الإشارة وإعادة إرسالها وهو يعمل في الطبقة الأولى من طبقات الـ OSI Layer والمعروفة بي Physical Layer وله نوعان Analog و Digital وله إستخدامات كثيرة مثل كوابل Copper-wire و كوابل الفايبر بالإضافة إلى شبكات الوايرليس

**HUBS** : أيضا جهاز خاص بالشبكات ويعمل على الطبقة الأولى من طبقات الـ OSI Layer ووظيفته ربط عدة أجهزة موجودة على نفس الشبكة ومن خلال Segment واحدة ببعضها البعض بالإضافة إلى ربط أجهزة تعمل بتقنيات مختلفة ببعضها البعض مثل twisted pair and coaxial cable وله ثلاث أنواع مختلفة : Passive Hubs, Active Hubs, Intelleents Hubs

**Bridge** : ومعناه باللغة العربية الجسر وهو جهاز مخصص لكي يعمل على الطبقة الثانية Data Link ووظيفته ربط الأجهزة الموجودة على الشبكة ببعضها البعض مستعينا بالعنوان الفيزيائي لكل جهاز Mac Adress وله نوعين Local Btidge و Remote Bridge

**SWITCH** : وباللغة العربية محول وهو أيضا أحد أجهزة الشبكة المعروفة وهو مخصص لكي يعمل على الطبقة الثانية وهناك سويتشات تدعم طبقات أعلى وتدعى Multilayer Switch وهو يقوم بنفس وظيفة الـ Bridge وما يميزه عن الجسر هو آلية نقل البيانات لان الأخير يعتمد على الـ Software في النقل أما السويتش فهو يعتمد على Application Specific Intergrated Circuits في النقل كما يعتبر السويتش MultiPort Bridge

**ROUTER** : وبالعربي موجه وهو يقوم بربط الشبكات ببعضها البعض ويعتمد على الأيبي في توجيه الترافيك لذا فهو يعد أحد أجهزة الطبقة الثالثة Network Layer ويدعم الشبكات القريبة Lan والشبكات البعيدة wan أما وظائفه فهي كثيرة جدا نذكر منه وصل الشبكات ببعضها البعض وفلترتها وتوجيهها نحو المكان الصحيح كما يقوم بمشاركة المعلومات التي لديه مع روترات أخرى ويمنع مرور الـ Broadcast من المرور الخ.... وهو يعد أبطلء من السويتش والبريدج بسبب اعتماده على طبقات أعلى .



# مشاكل وحلول

سوف يتم تخصيص هذا القسم لعرض المشاكل التي قد تواجهك في الشبكة بالإضافة إلى طريقة حل المشكلة كما أرحب أيضا بأرسال مشاكلكم على بريد المجلة [magazine@networkset.net](mailto:magazine@networkset.net) للنظر فيها وتقديم أفضل الحلول لها .

سؤال: ما أهمية الـ Process-id في الـ OSPF ؟

للإجابة على هذا السؤال يجب أن نعرف أن الـ Procsee ID في الـ OSPF لا يتعلق بباقي الروترات وهو خاص بي الروتر لوحده وبمعنى آخر local to the router only أي أن روتران في نفس الأريا سوف يعملان حتى لو كان الـ Process id مختلف وهي تفيد في حال كان الروتر يملك multiple OSPF على نفس الروتر ونريد أن تكون كل عملية منعزلة عن الأخرى لذا نلجأ لأعطاء كل عملية منها ايدي مختلف عن الآخر والرانج الخاص بها يبدأ من واحد وينتهي بي 65535 والأمر يكتب على الشكل التالي Router OSPF 3 وطبعا الأمر مختلف في EIGRP لان الـ Process id هناك يجب ان يكون موحد على كل الروترات

سؤال: ماهو local port and remote port وماهو الفرق بينهم ؟

جواب: عند دراستك الـ OSI Layer وخصوصا في الطبقة الرابعة Transport Layer سوف تجد جوابك وبشكل عام هذه الطبقة كما هو معروف عنها أنها تقوم بتحديد نوع البروتوكول المستخدم TCP أو UDP بالإضافة إلى وظائف أخرى وطريقة الاختيار ترجع إلى نوعية التطبيق الذي تستخدمه فإذا كنت تستخدم تطبيق الـ HTTP وتريد ان تتصفح أحد المواقع فأنت تستخدم أحد البورتات العشوائية الموجودة عندك للاتصال مع البورت 80 وكما هو معروف ان عدد البورتات هو 65536 أول 1023 بورت محجوز لخدمات معينة مثل http,ftp,dns,dhcp الخ .... وباقي البورتات تعتبر للاستخدام العام فمنها من يستخدم لبعض البرامج مثل الماسنجرات أو اي برنامج يتطلب استخدامه الأنترنت لذا الفكرة ببساطة هي ان الـ local Port هو الـ Source Port الذي يتم كتابته في الهيدر الخاص بي الـ TCP او الـ UDP بينما الـ Remote Port هو الـ Destination Port فعندما تتصفح الأنترنت أو اردت طلب صفحة معينة فأنت تضع في الهيدر الخاص بي الـ TCP رقم بورت عشوائي وليكن 1025 وهو يمثل السورس بورت أو لوكال بورت بينما تضع البورت 80 ليكون هو الـ ريموت بورت أو الـ Destination Port والسبب يعود كون التطبيق الخاص بي الـ HTTP في السيرفر الي يحوي الموقع يكون مفتوح على البورت 80 ويتسمع على انواع الترافيك الذي يصل اليه وعندما يصل الطلب سوف ينظر الى الهيدر ليكتشف أن هذا الطلب قادم لخدمة الـ HTTP فيأخذ الطلب ويضع المطلوب بداخله ويعيد ارساله لكن هذا المرة سوف يرد بان يضع اللوكال بورت رقم عشوائي بينما الـ ريموت بورت سوف يكون 80

مشكلة: انا عندى فى الشغل روتر سيسكو 1841 وأريد أن طريقة أقوم بوصل الأنترنت مع الروتر من خلال مودم DSL فماهي الأعدادات اللازمة للقيام بهذا الموضوع ؟

الحل: كل ما عليك ان تقوم به على الروتر هو الـ default route للشبكة من خلال الأمر ip route 0.0.0.0 0.0.0.0 192.168.1.1 ويكون أيبى المودم وبعدها اتجه إلى السويتش وقم بكتابة الأمر التالي ip default-gateway 172.16.1.1 والايبي طبعا خاص بالمنفذ الموجود على الروتر والممتل مع السويتش (الخطوة الثانية تقوم بعملها في حال كان السويتش عندك قابل للأعداد ) ملاحظة صغيرة تقنية الـ PAT مفعلة على الروتر By Default